POURQUOI LES CEO NE DORMENT PAS?

YVES PAQUETTE
Co-Fondateur et Président
NOVIPRO

DOMINIQUE DERRIER
CISO - NOVIPRO
Président - ASIMM

CONFÉRENCE CYBER SÉCURITÉ 2020

ÉDITION VIRTUELLE

NOVIPRO

ÉTUDE NOVIPRO/LÉGER – 5E ÉDITION

L'ANNÉE DU GRAND BOULEVERSEMENT

40 %

DES ENTREPRISES ONT RÉDUIT LEURS INVESTISSEMENTS EN SÉCURITÉ

- → Diminution marquée des investissements en sécurité
- → Déploiement de projets d’intelligence artificielle freinés
- → Hausse de la perception de vétusté des équipements technologiques

ALORS QUE DES TENDANCES SE DESSINAIENT DEPUIS 2016, LA COVID-19 A CHAMBOULÉ LES PLANS DES ENTREPRISES.

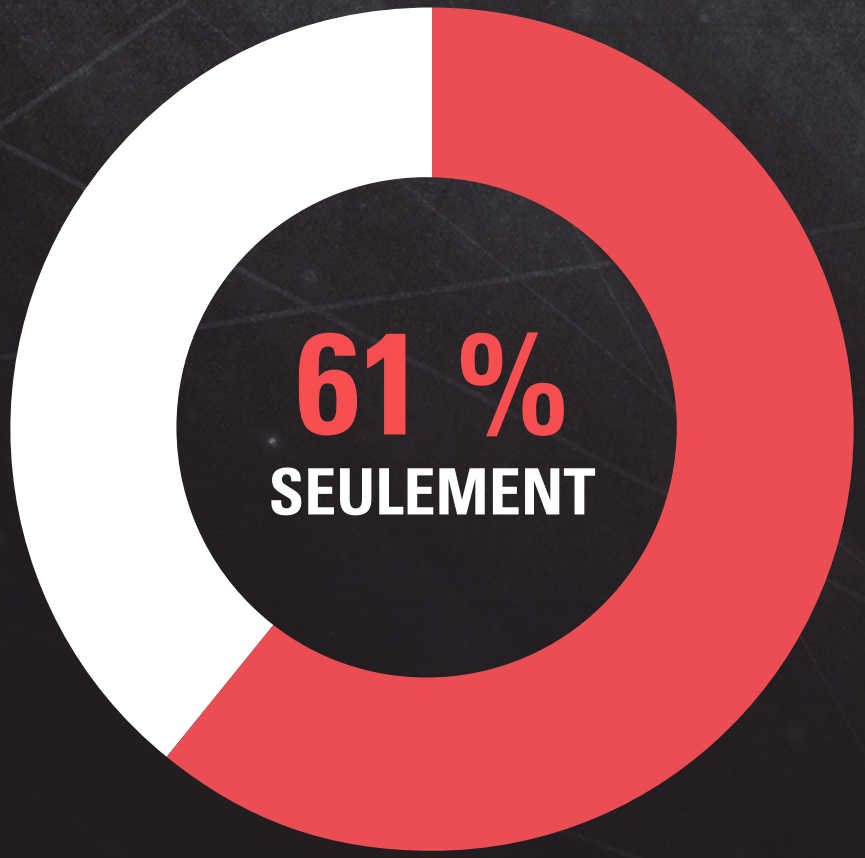
DIMINUTION MARQUÉE DES INVESTISSEMENTS EN SÉCURITÉ

→ **81 %** des entreprises affirment que la pandémie les a amenés à revoir leurs pratiques en matière de sécurité.

→ Néanmoins, **seulement 25 %** des entreprises planifient investir en solutions de sécurité d'ici les deux prochaines années alors que le télétravail accroît les risques de menaces informatiques.

Diminution de 40 %

par rapport à 2019



PLAN DE CONTINUITÉ

Seulement 61 % des entreprises ont un plan de continuité des affaires.

RESPONSABLE DU PLAN DE CONTINUITÉ DANS LES ENTREPRISES CANADIENNES :

- → 59% Direction
- → 32% Équipe TI
- → 9% CISO

COÛT DES ATTAQUES

Plus du tiers des entreprises affirment qu'une cyberattaque leur a coûté entre 50 000 $ et 250 000 $ (considérant le coût de la menace informatique, des ressources additionnelles et des pertes occasionnées)

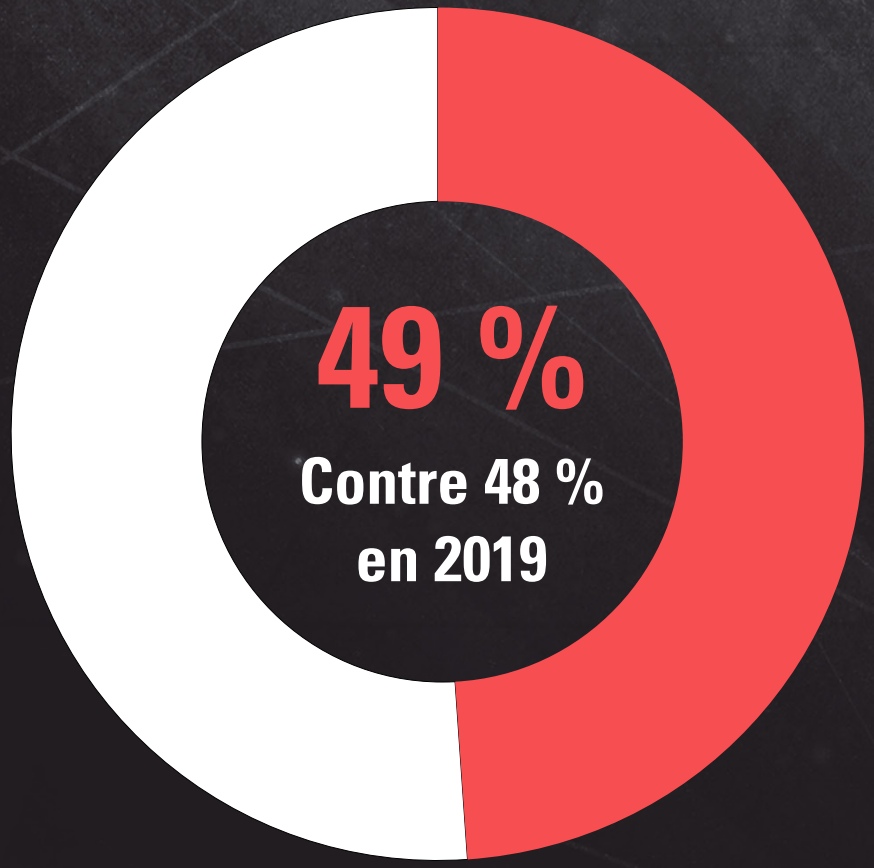
→26 % moins de 50 000 $

→**35 % entre 50 000 $ et 250 000 $**

→25 % entre 250 000 $ et 500 000 $

→9 % entre 500 000 $ et 1 million

→5 % + de 1 million



DES LEÇONS À ASSIMILER

Globalement, les organisations ne semblent pas intégrer certaines leçons liées à la protection de leurs données.

Seulement la moitié (49 %) des entreprises indiquent que les nouvelles médiatiques liées aux fuites de données chez les entreprises les ont amenées à revoir leur pratique, ce qui est autant que l'année passée (48 %)

LES ENTREPRISES MAL ÉQUIPÉES CONTRE LES CYBERATTAQUES

Malgré l'actualité chargée en nouvelles sur les entreprises victimes de cyberattaque, moins d'organisations semblent être visées cette année comparativement à la dernière étude (21 % au lieu de 37 %).

39 %
Pertes de données

36 %
Vols de données

38 %
Intrusions

37 %
Virus

FORMATION

Moins d'entreprises que l'année dernière ont offert une formation en sécurité à leurs employés au cours de la dernière année

→ 69 % cette année comparativement à 74 % lors de notre dernier sondage

→ Elles sont aussi moins nombreuses à vouloir en offrir une l'année prochaine : **42 % vs 51 % lors du dernier sondage**

C'est au Québec qu'on a le moins formé les employés en sécurité (61 %), comparativement à :

70 %
ONTARIO

75 %
ATLANTIQUE

77 %
PRAIRIES

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

TRANSITION VERS UNE ÉCONOMIE CYBERSÉCURITAIRE

STEVE WATERHOUSE
Professionnel en cybersécurité

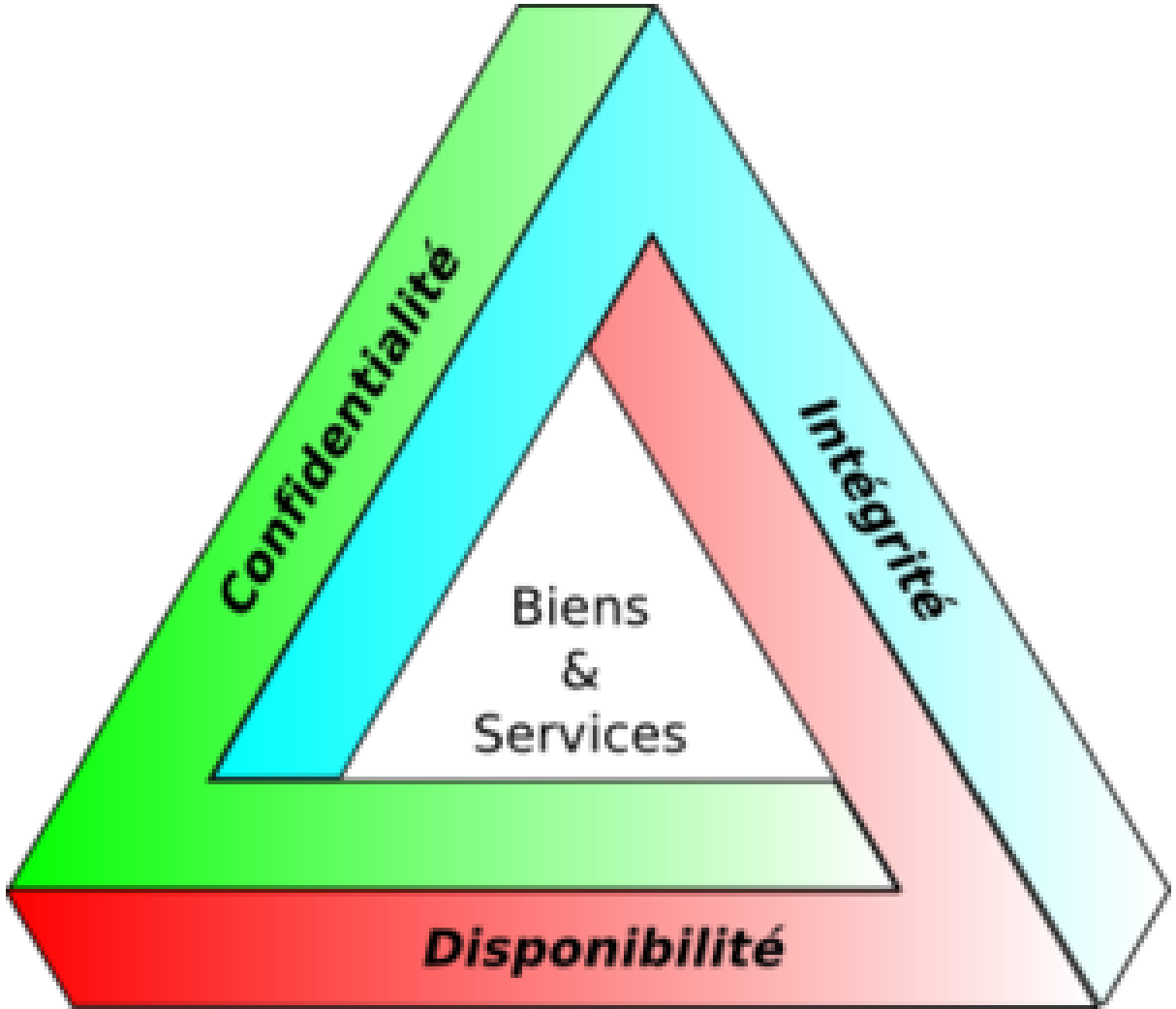
CONFÉRENCE
CYBER
SÉCURITÉ
2020
ÉDITION VIRTUELLE

TRANSITION VERS UNE ÉCONOMIE CYBERSÉCURITAIRE
PLAN DE PRÉSENTATION

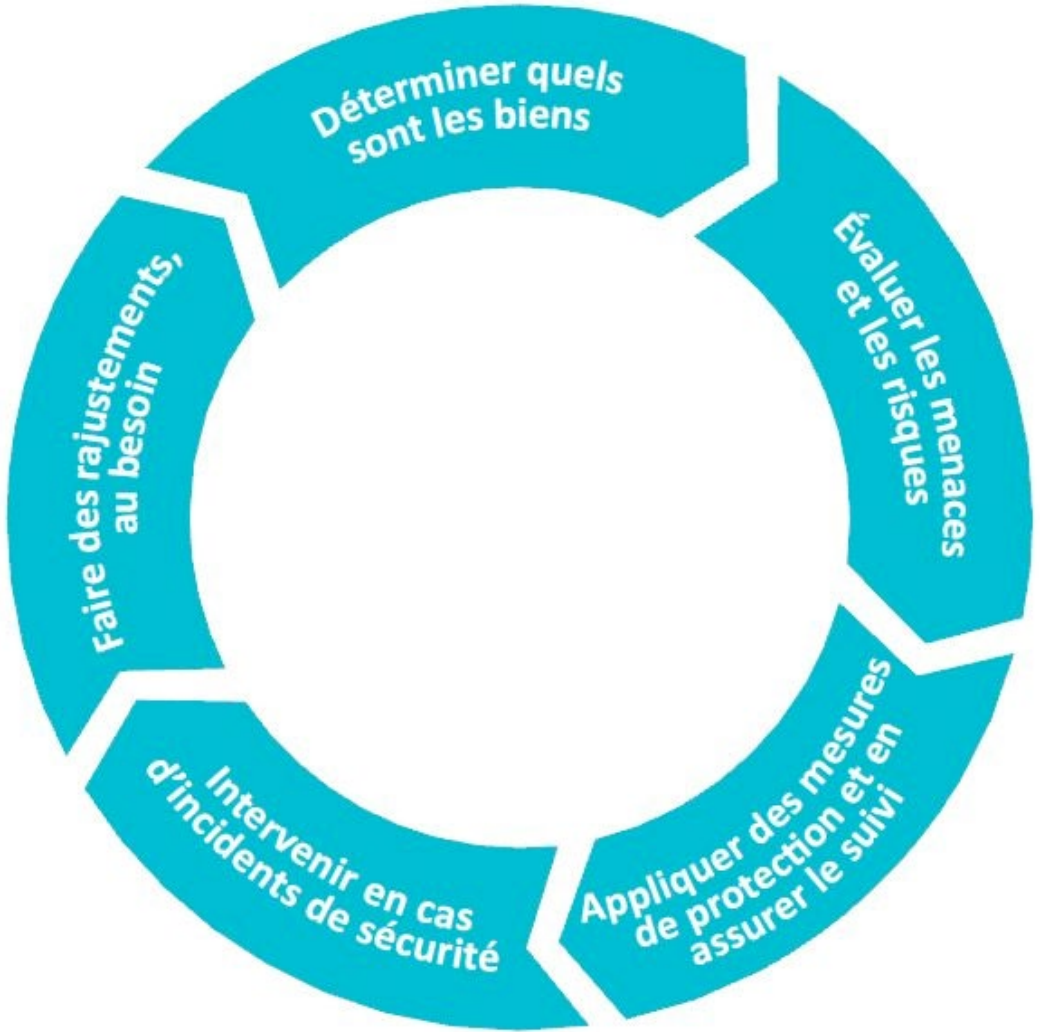
- Contexte de la présente situation
- Connaissez-vous la sécurité de l'information ? (INFOSEC)
- Les menaces actuelles ?
- Exemples comment ça va pas bien
- Différents types de pirates informatique
- Ces mots de passe maudit
- Classification de l'information
- Solutions éducatives
- Initiatives du Gouvernement du Canada
- Initiatives du Gouvernement du Québec
- Conclusion

CONNAISSEZ-VOUS LA SÉCURITÉ DE L'INFORMATION ? (INFOSEC)

SÉCURITÉ DE L'INFORMATION (INFOSEC)



PRINCIPES FONDAMENTAUX

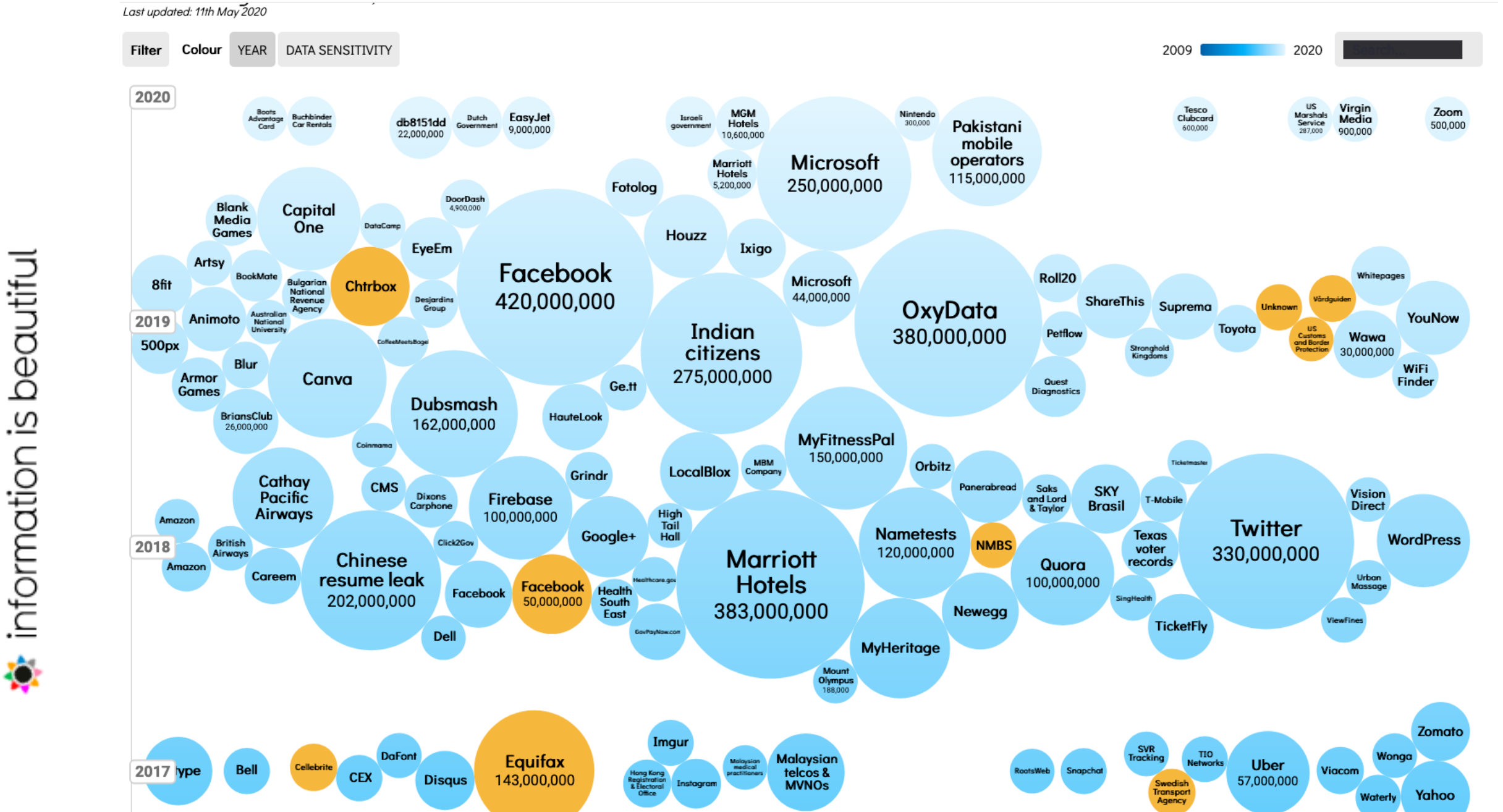


IL N'Y A PAS DE FRONT DANS LA CYBERSÉCURITÉ
UNE MISE À JOUR DU MODÈLE S'IMPOSE

"In cyber security there is no front line"
- An update to the Cyber Security Model

CYBERSECURITÉ

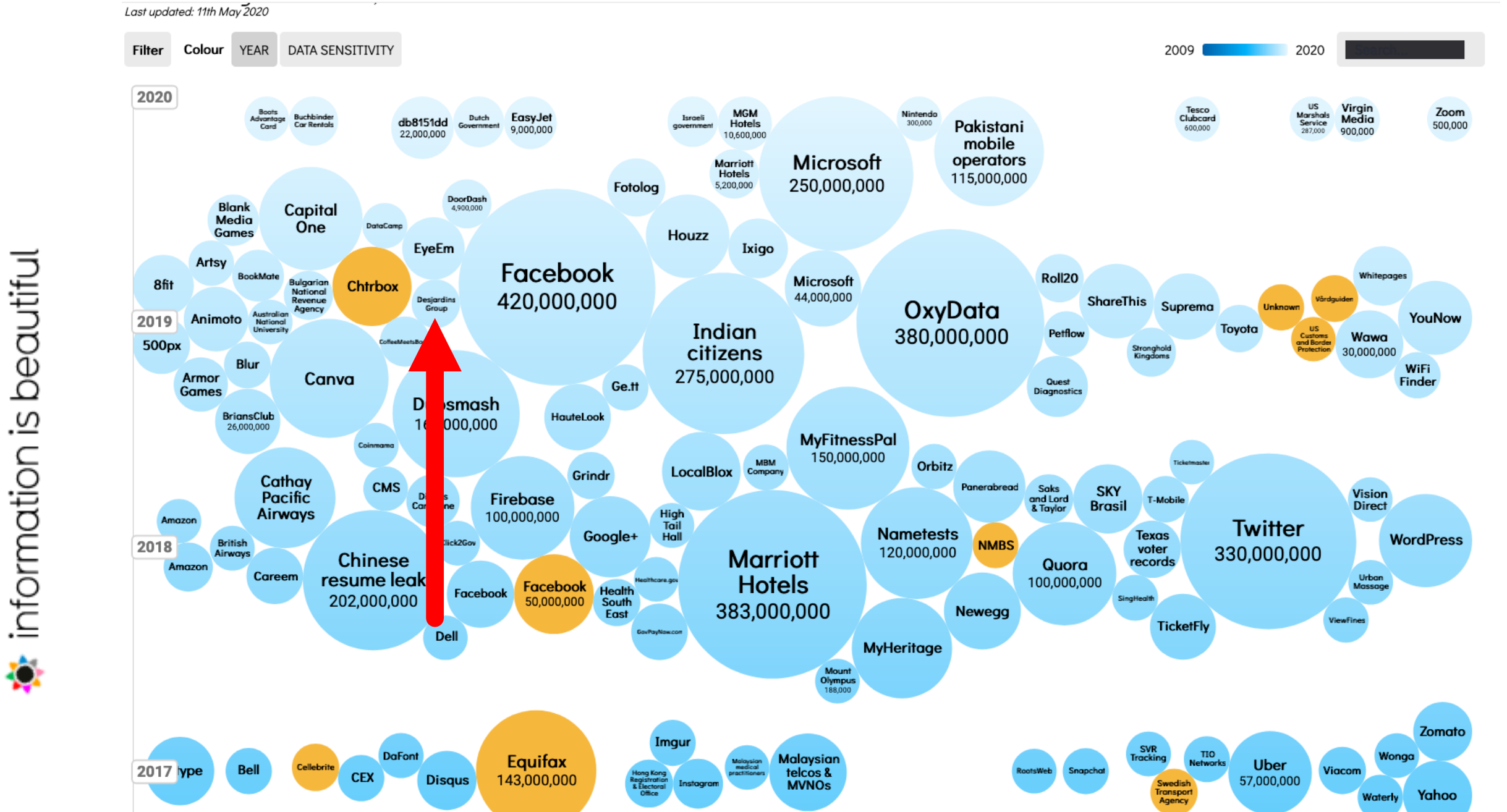
Prévenir ces situations qu'elles arrivent



information is beautiful

CYBERSECURITÉ

Prévenir ces situations qu'elles arrivent



information is beautiful

LES MENACES ACTUELLES ?

CONTEXTE DE MENACE ACTUEL

- Cyberattaques sont:
  - Peu coûteuses
    - Maintenant en format cloud !
    - $10/h pour service de DDoS
  - Efficaces
    - Y a tellement de failles…
    - Étalement des vulnérabilités
    - Augmentation des surfaces d'attaque
  - Peu risquées (anonyme)
    - Retracer un pro est quasi impossible
    - Peu de journalisation

SONDAGE 2018 DE LA SÉCURITÉ DE L'INFORMATION GLOBAL 2017-2018 - EY

SONDAGE 2018 DE LA SÉCURITÉ DE L'INFORMATION GLOBAL 2017-2018 - EY

100%

des répondants disent qu'Ils ont besoin d'augmenter de 50% leur budget en cybersécurité

80%

des répondants considèrent que ce sont des employés négligents qui sont probablement la source des attaques

65%

n'ont pas, ou on seulement un programme informel de renseignement de la menace

91%

Disent leur fonction de cybersécurité ne rencontre pas pleinement le besoin organisationnel

58%

N'ont pas de Centre des Opérations de Sécurité (SOC) malgré qui soient de plus en plus communs

common.

17%

des conseils (CA) ont suffisamment de connaissances en cybersécurité pour une supervision du cyber-risque

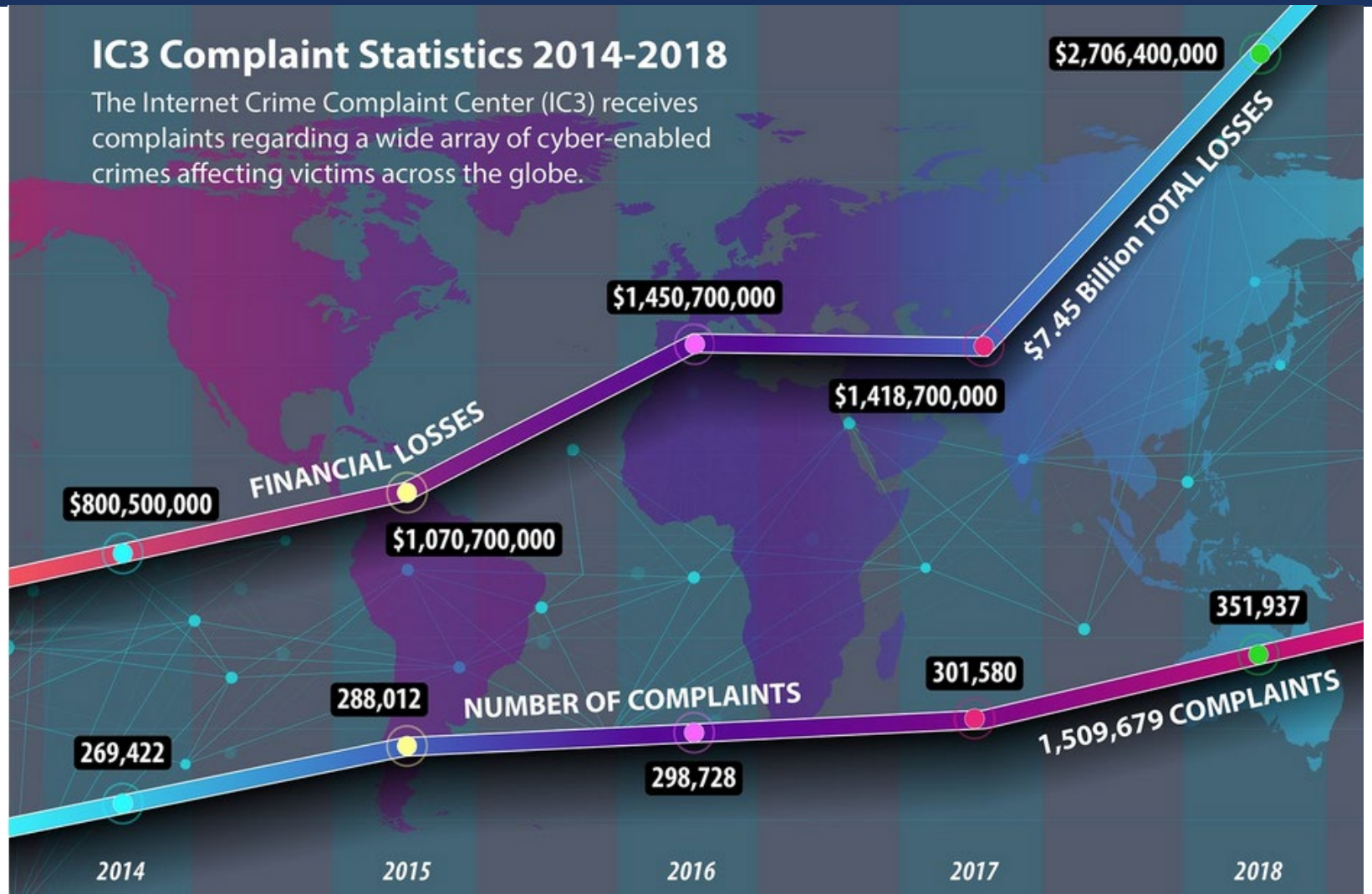
14%

sont d'avis qu'il seraient très probable en mesure de détecter une cyberattaque sophistiquée

76%

des organisations gardent toujours les rapports de cybersécurité principalement dans une fonction de TI

FBI - CYBER-CRIME ET AUGMENTATION DES COÛTS 2018



2019

Dossier documentaire sur internet au canada

https://www.cira.ca/fr/resources/corporation/dossier-documentaire/canadas-internet-factbook-2019

2019
LE GUIDE DE L'INTERNET AU CANADA

SEULS

15 %

affirment être restés hors ligne pendant au moins une semaine ou plus au cours de la dernière année.

acei

2019
LE GUIDE DE L'INTERNET AU CANADA

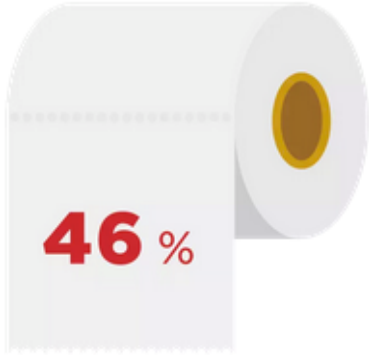
UN CANADIEN sur 5

déclare **ne jamais passer plus de huit heures** sans se connecter au réseau Internet.

acei

2019
LE GUIDE DE L'INTERNET AU CANADA

des Canadiens admettent naviguer sur Internet lorsqu'ils **regardent la télévision.**

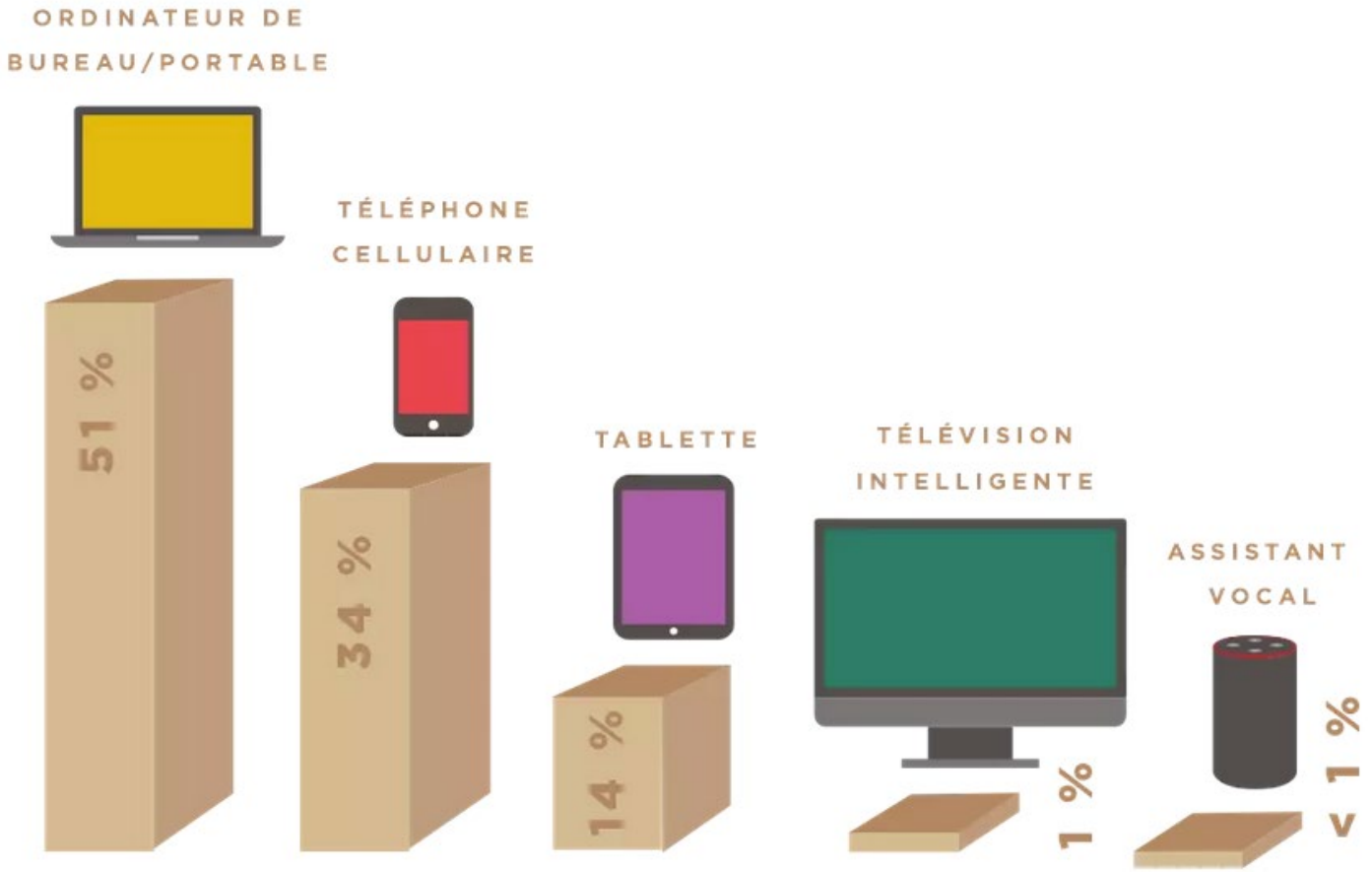


admettent utiliser leur téléphone lorsqu'ils **vont aux toilettes.**

Près des **3/4** des Canadiens passent au moins **3 à 4 heures** en ligne par jour.

acei

2019
LE GUIDE DE L'INTERNET AU CANADA



acei

Comment les Canadiens accèdent-ils à Internet?

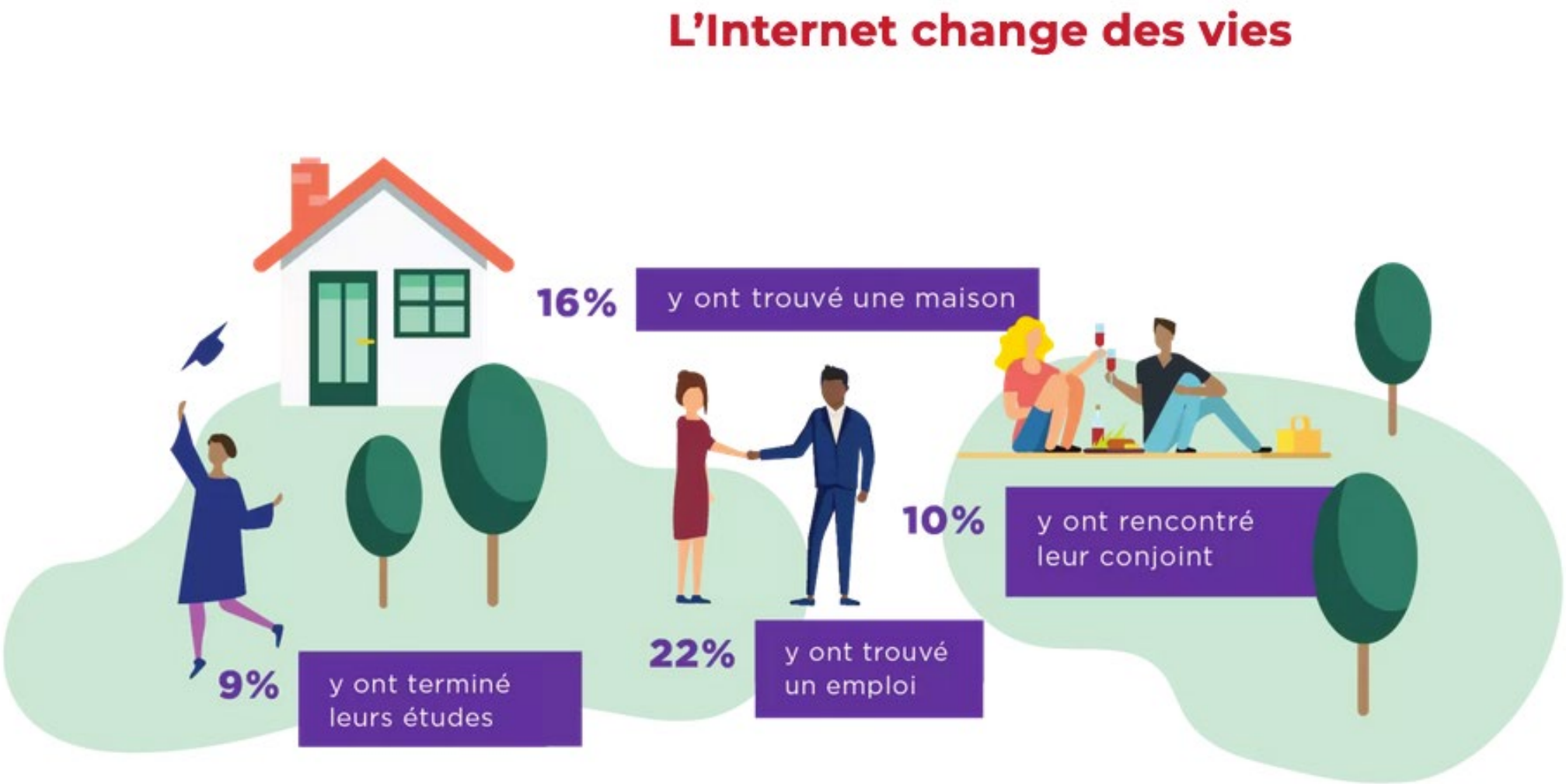
2019
LE GUIDE DE L'INTERNET AU CANADA

(55 ans +) naviguent sur le Web à partir d'appareils mobiles –

57 % en 2019 vs. **24 %** en 2015.

acei

2019
LE GUIDE DE L'INTERNET AU CANADA



2019
LE GUIDE DE L'INTERNET AU CANADA

*données seulement disponibles pour quatre ans

acei

2019
LE GUIDE DE L'INTERNET AU CANADA

64 % des Canadiens préfèrent **acheter en ligne** auprès d'un **détaillant canadien**

JE CHOISIS

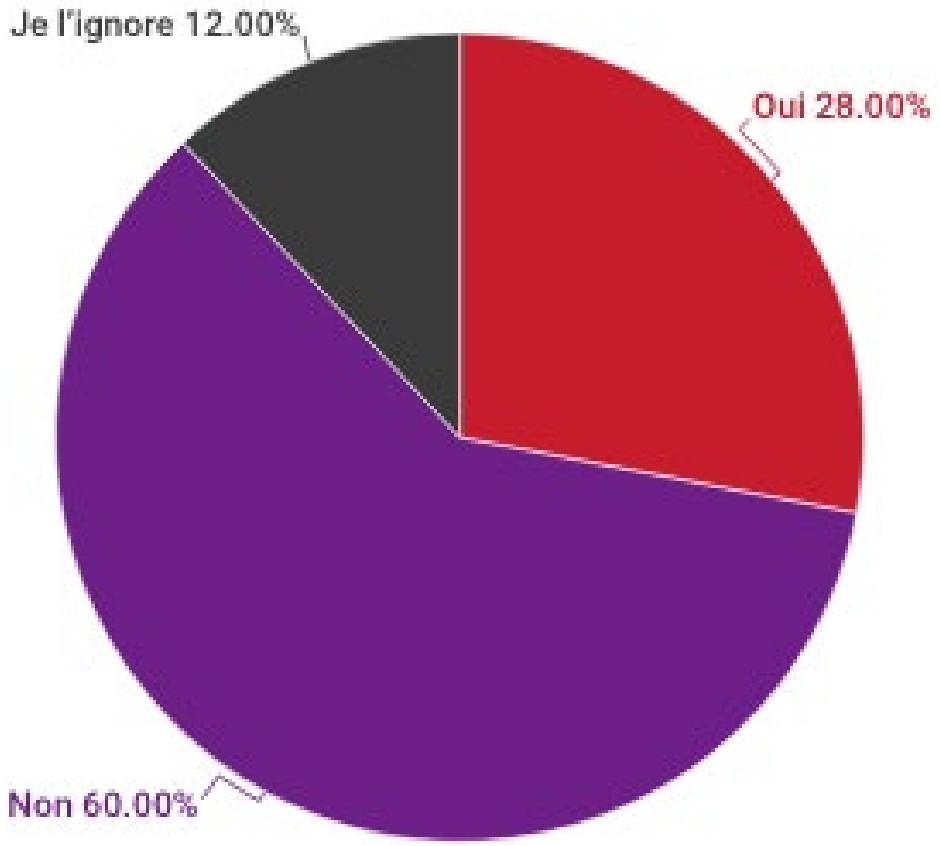
.CA

acei

https://www.cira.ca/fr/cybersecurity-report-2020

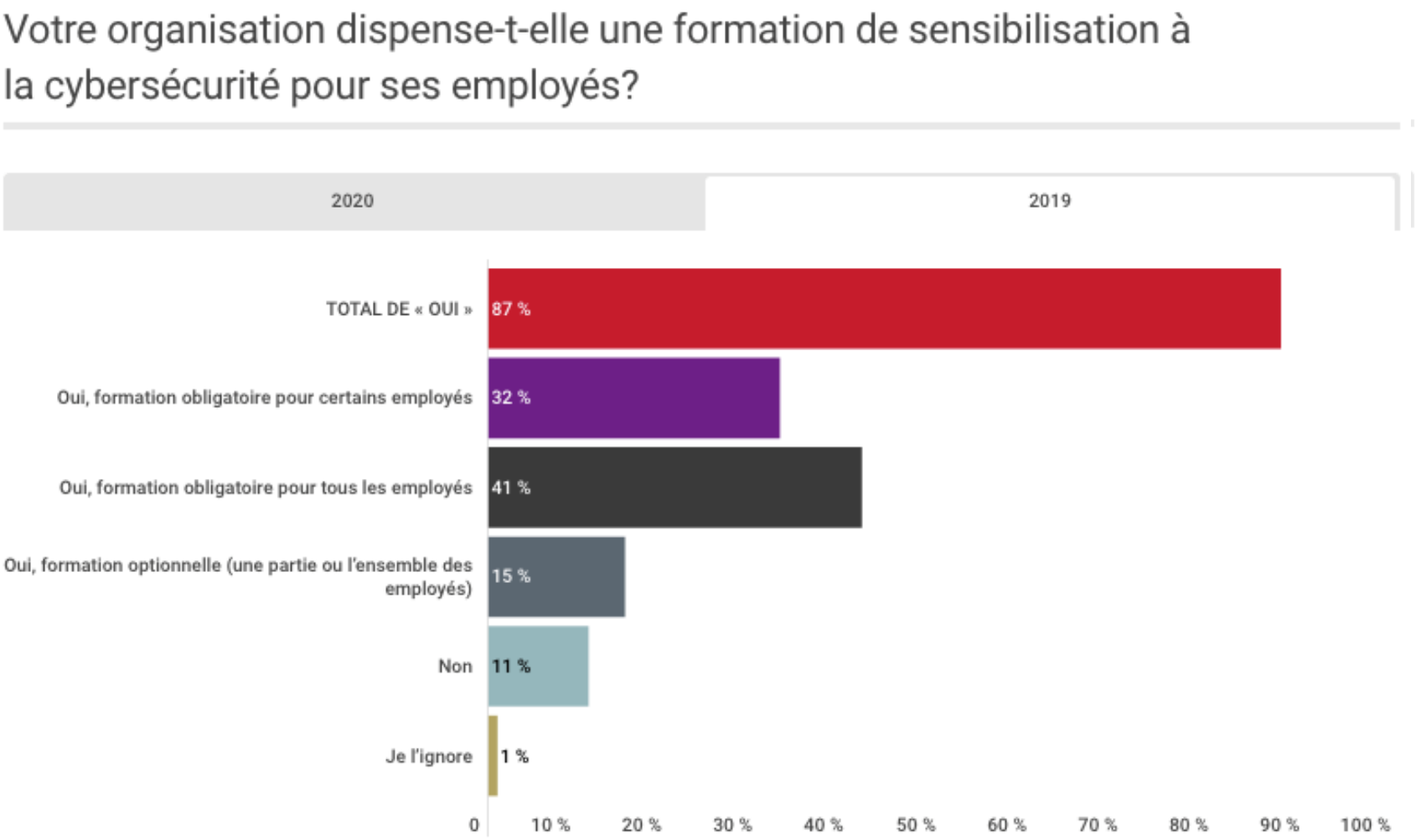
RAPPORT SUR LA CYBERSÉCURITÉ DE 2020 DE L'ACEI

Votre organisation a-t-elle été ciblée par un incident de cybersécurité ayant pour thème la COVID-19?

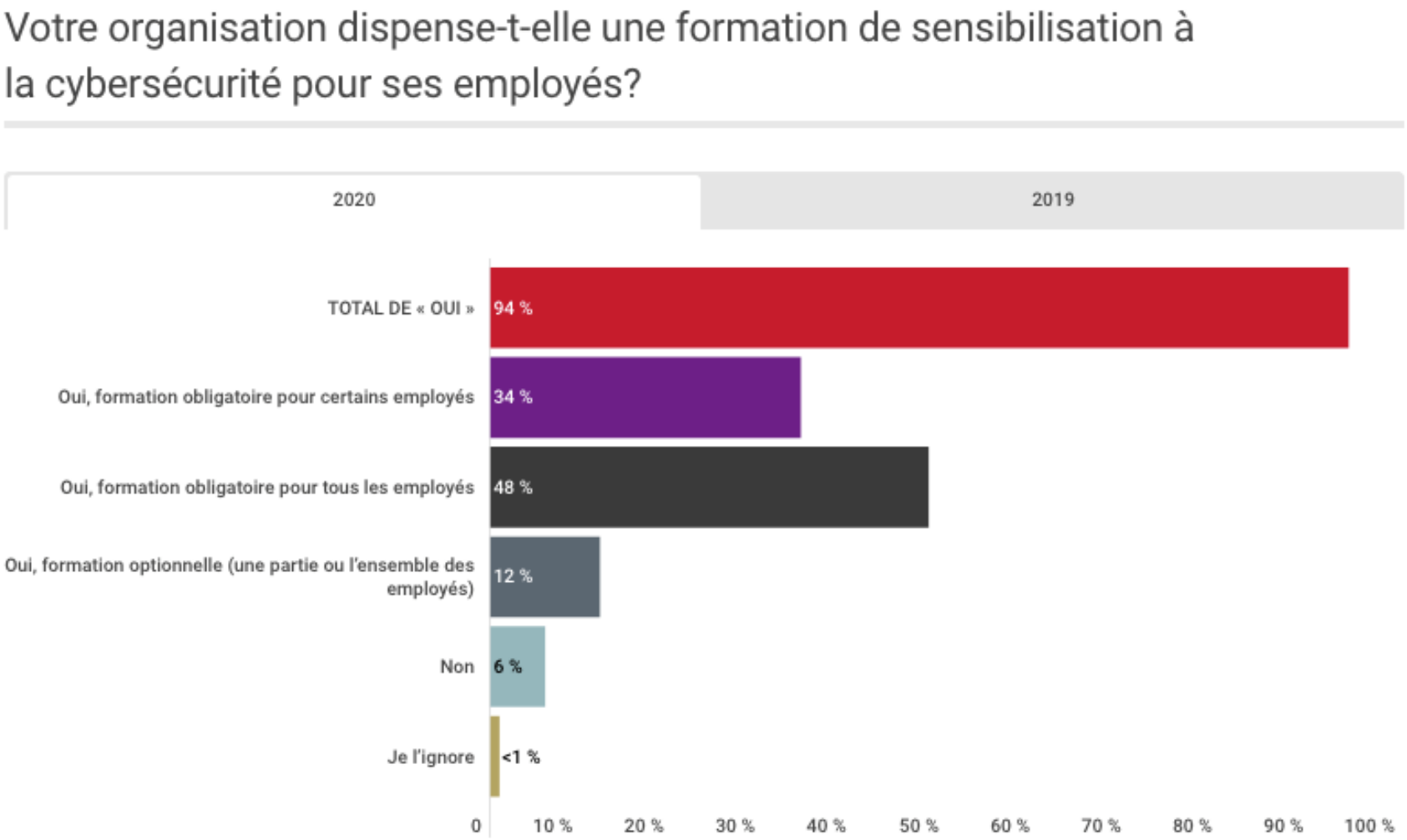


acei

RAPPORT SUR LA CYBERSÉCURITÉ DE 2020 DE L'ACEI

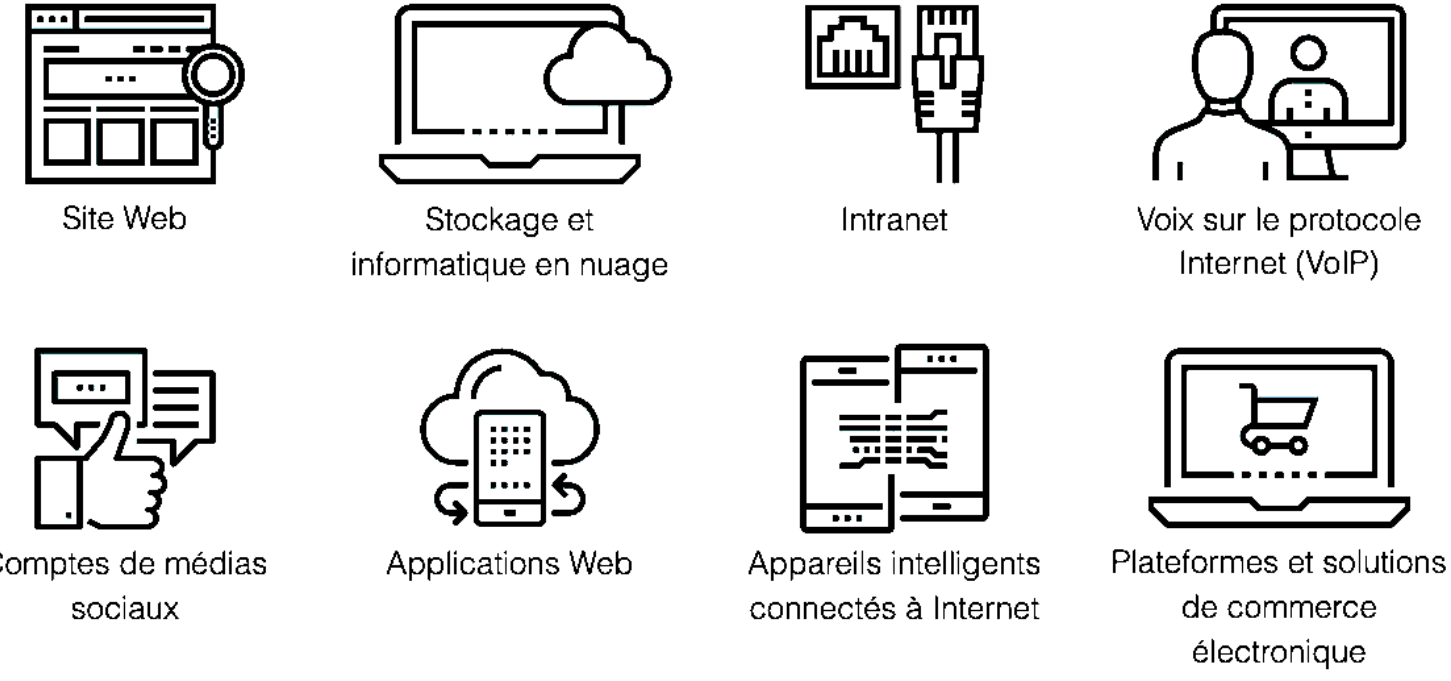


RAPPORT SUR LA CYBERSÉCURITÉ DE 2020 DE L'ACEI



QU'EST-CE QU'UN ENVIRONNEMENT DES CYBERMENACES?

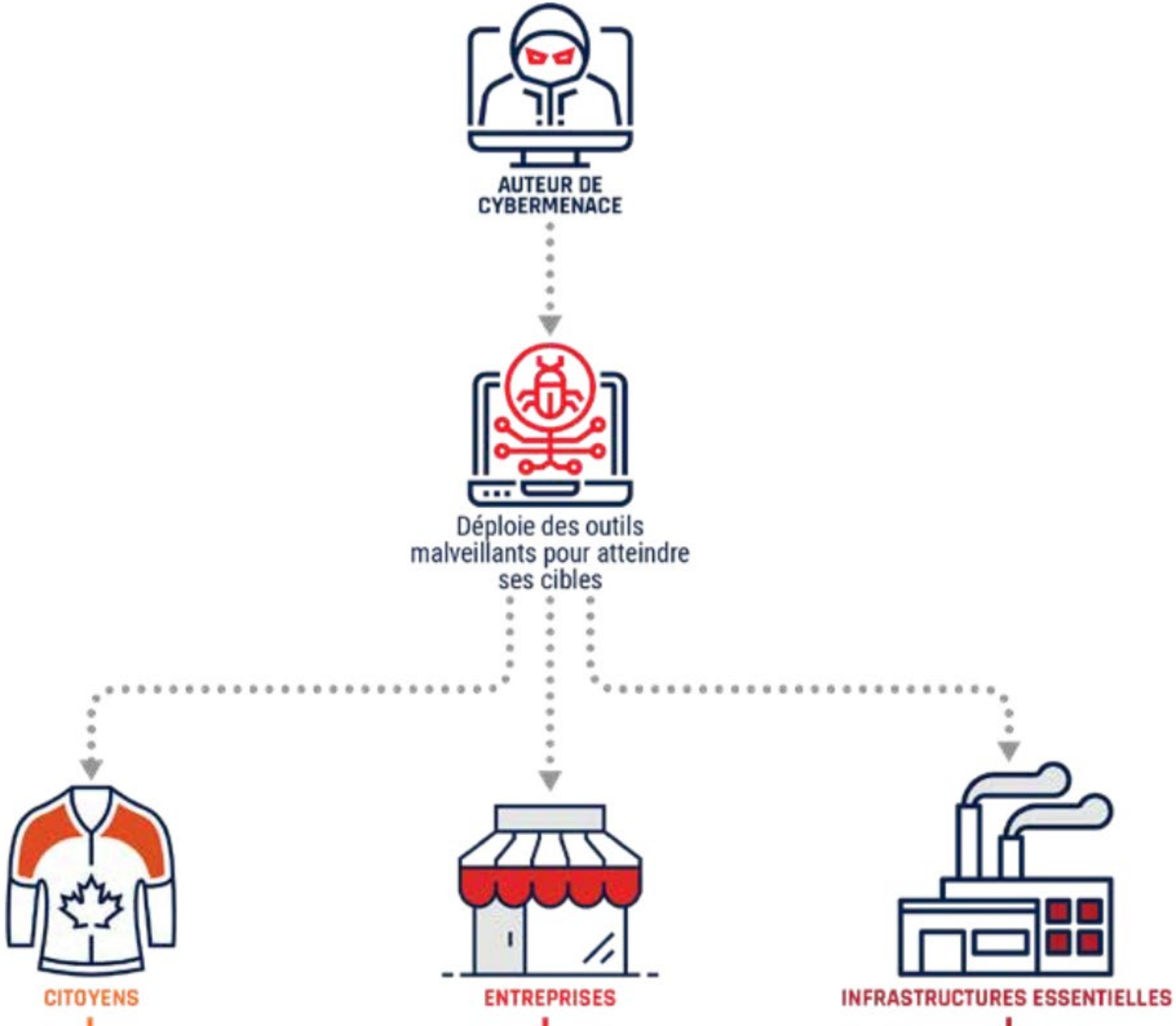
Un **environnement des cybermenaces** est l'espace en ligne au sein duquel peut se tramer l'activité malveillante de cybermenace.



Innovation, Sciences et Développement économique Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

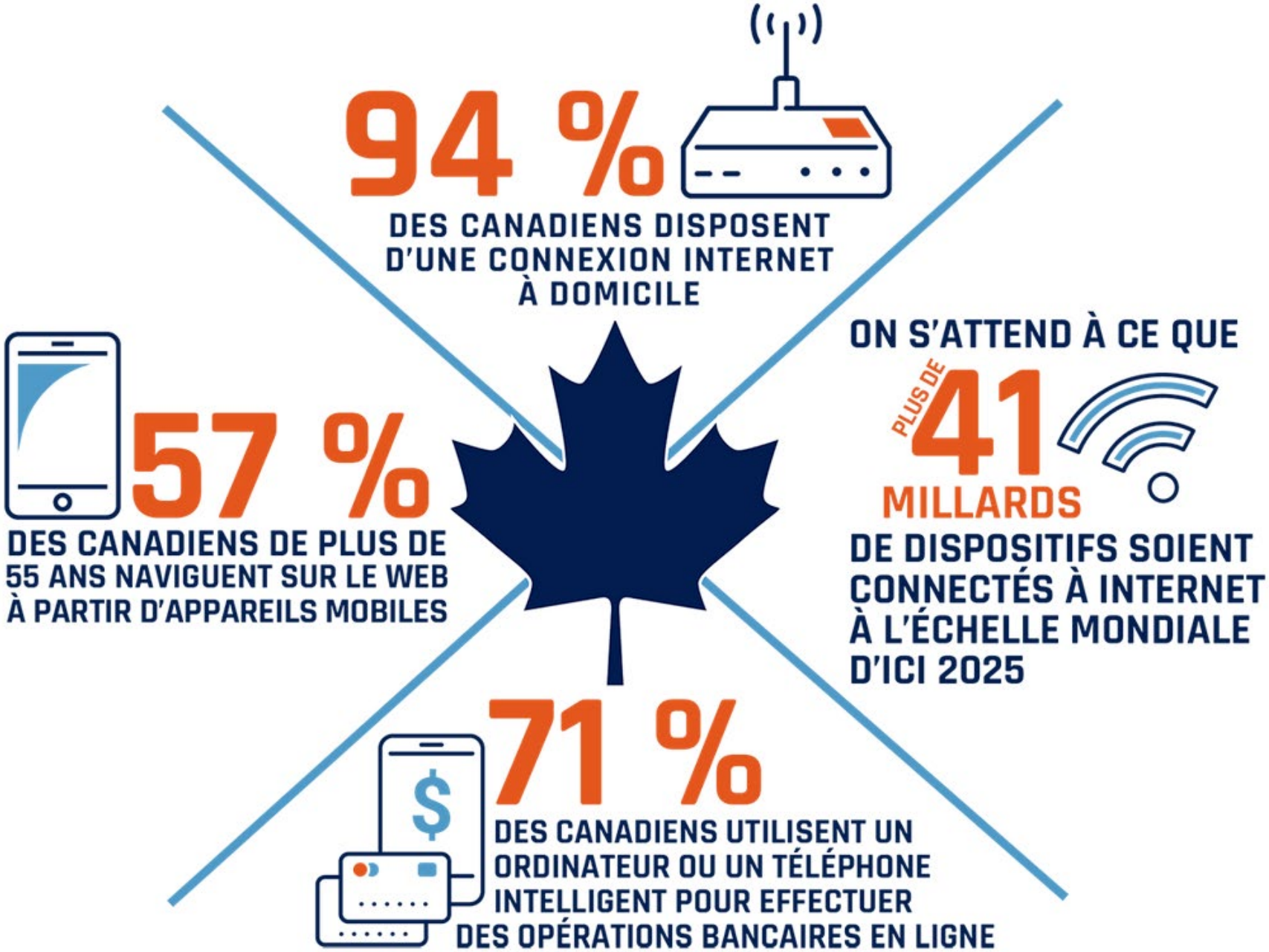
ÉVALUATION CYBERMENAC NATIONALES 2018



CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

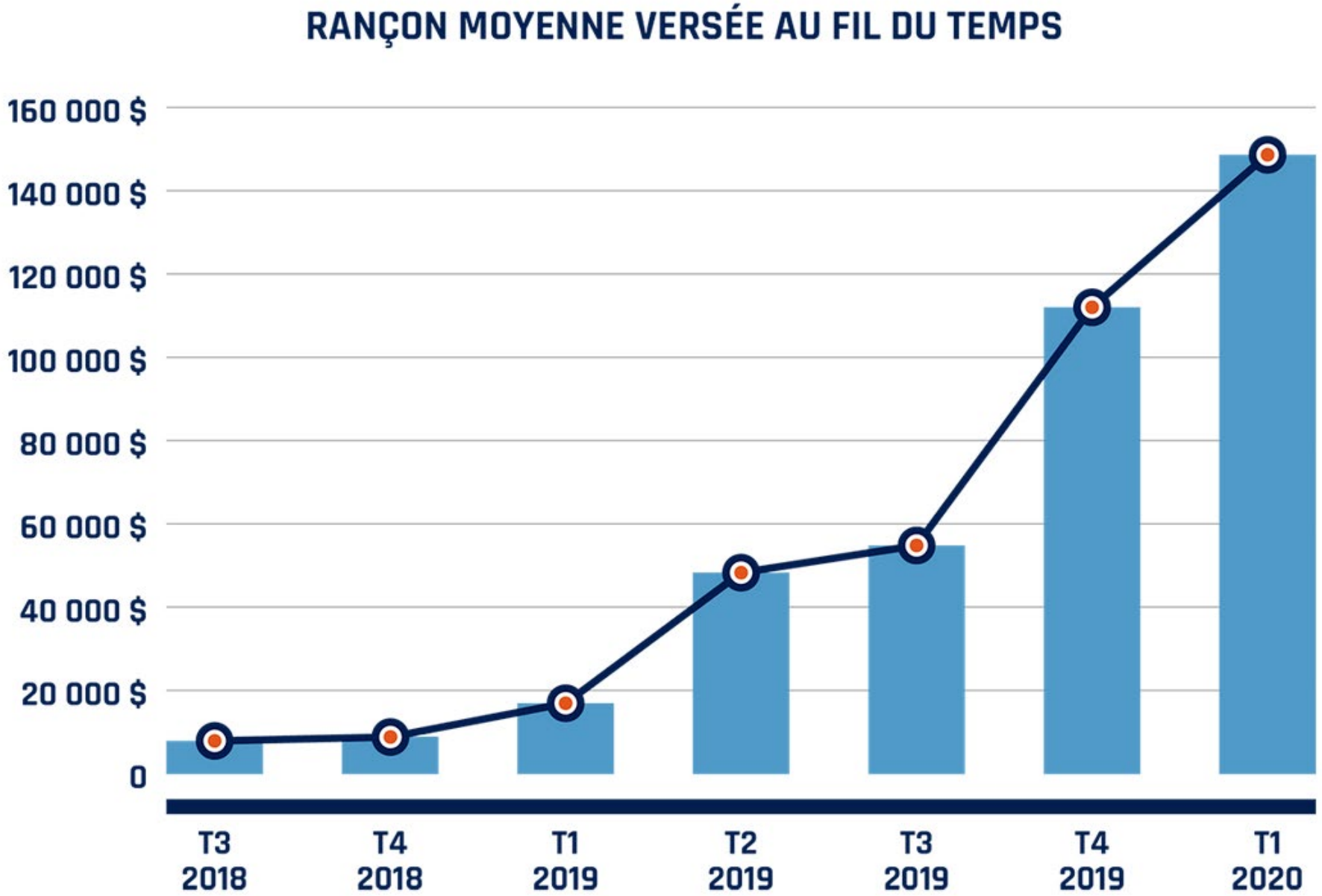
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020



CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020

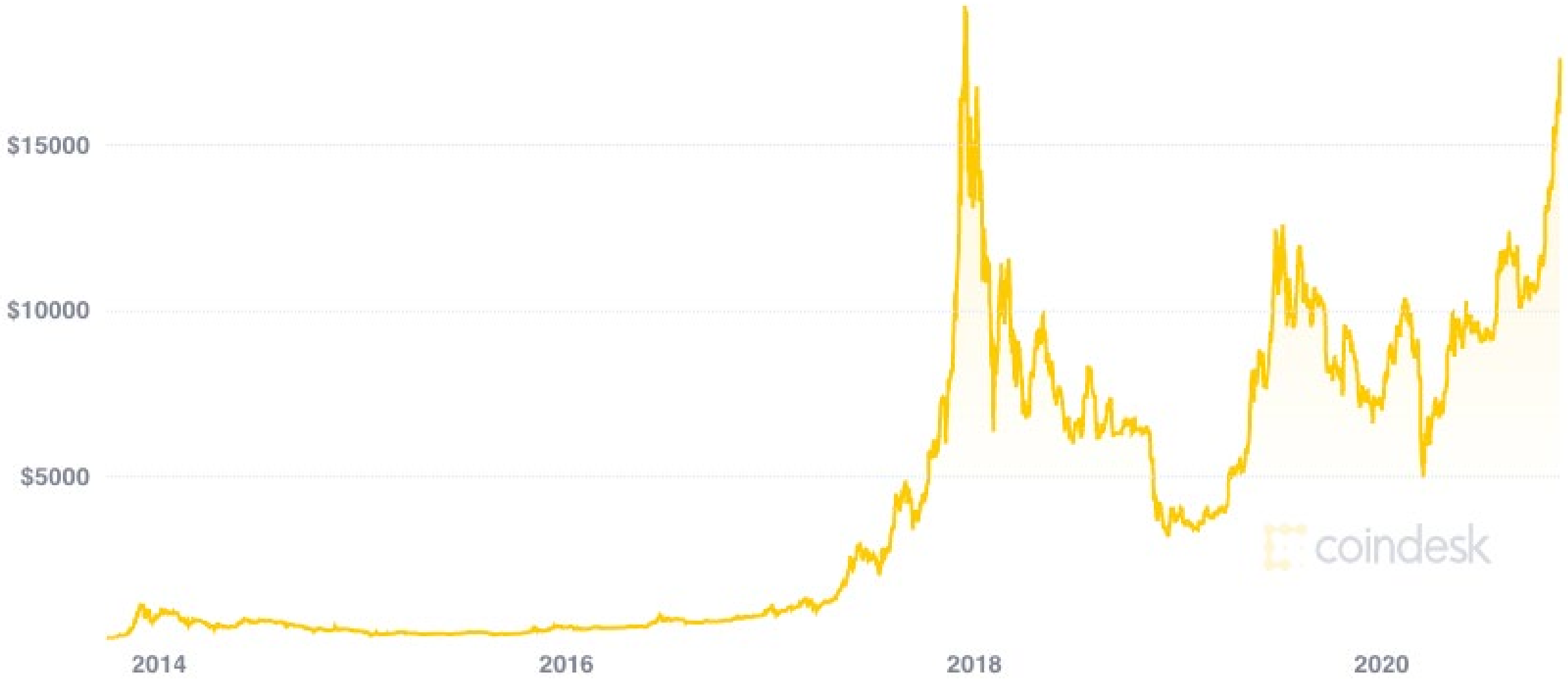


CANADIAN CENTRE FOR CYBER SECURITY

https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020

07/18/2010 to 11/18/2020

1h 12h 1d 1w 1m 3m 1y all



EXEMPLES COMMENT ÇA VA SI MAL

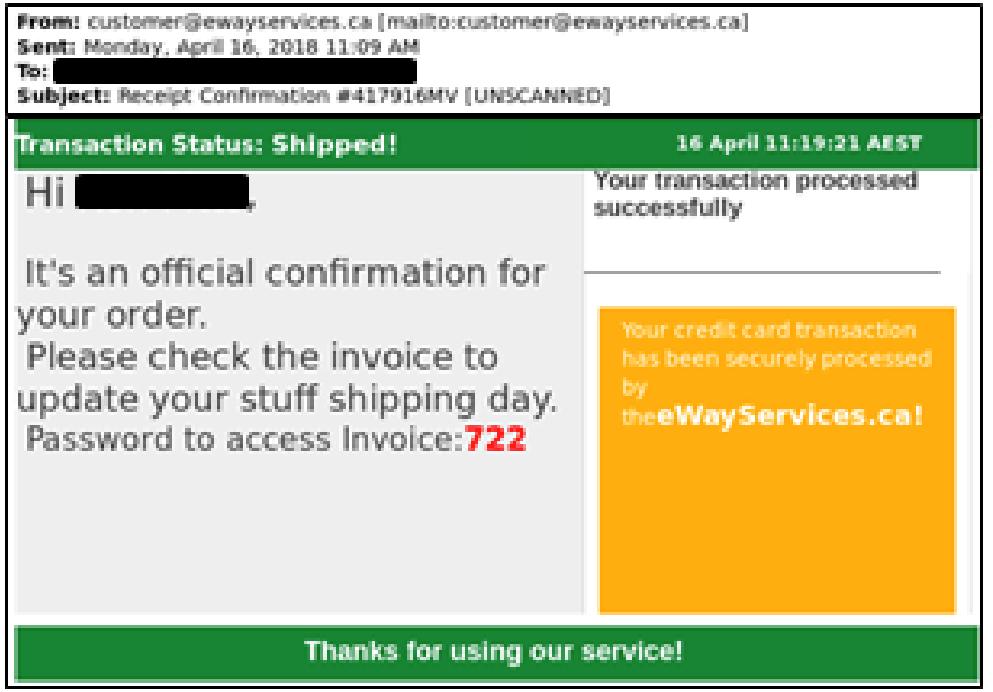
THE CYBER KILL CHAIN

Typical scenario of a cyberattack nowadays (APT)

Forcepoint (Websense)

LE MALWARE EMOTET

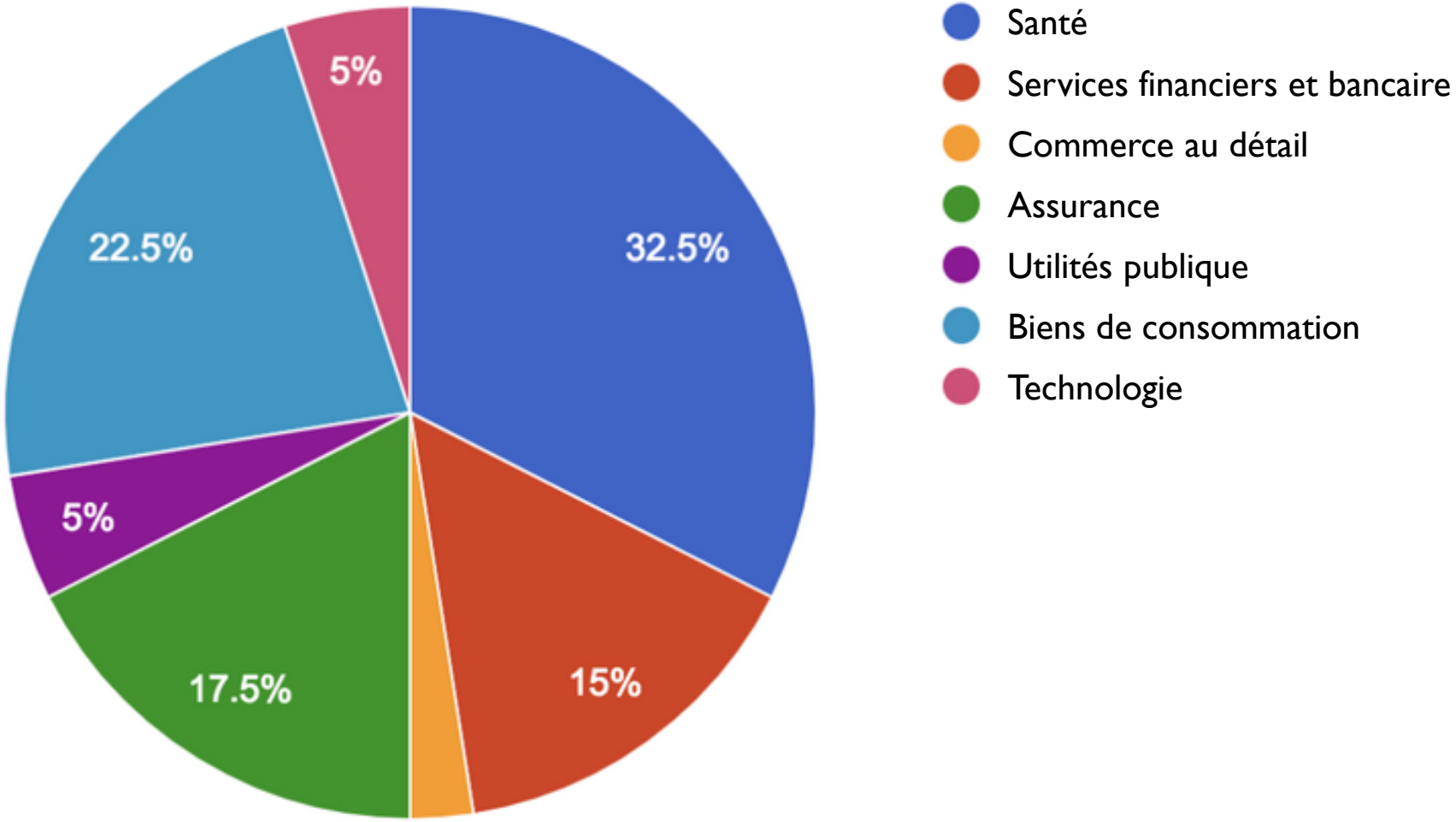
- À l'été 2014, le vers informatique Emotet fait ses débuts
- Secteur financier initialement ciblé
- Vulnérabilité des systèmes Windows exploités
- Noms de variante de vers utilisés
  - IcedID banking Trojan,
  - Trickybot,
  - Ransom.UmbreCrypt, et
  - Panda Banker.
- Juillet 2019: Emotet a maintenant 30,000+ variantes



LE MALWARE EMOTET

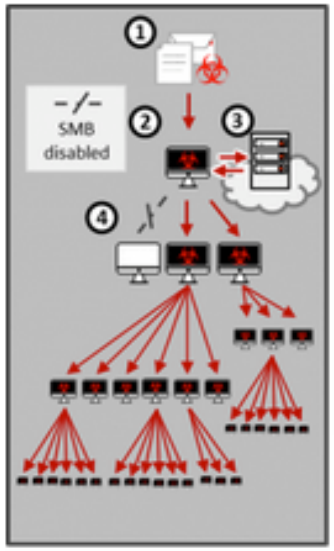
Début 2019

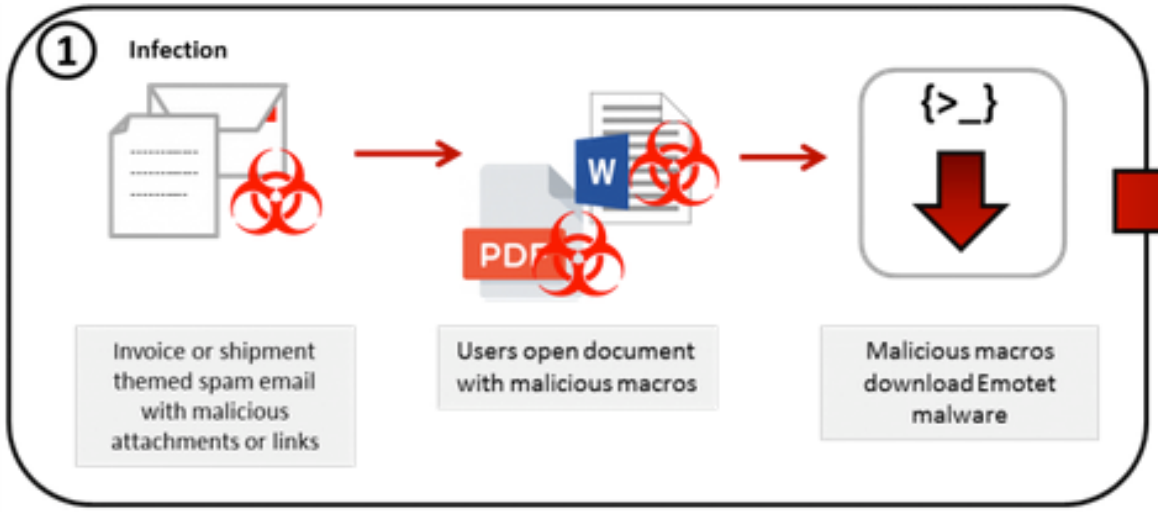
Secteurs d'activité

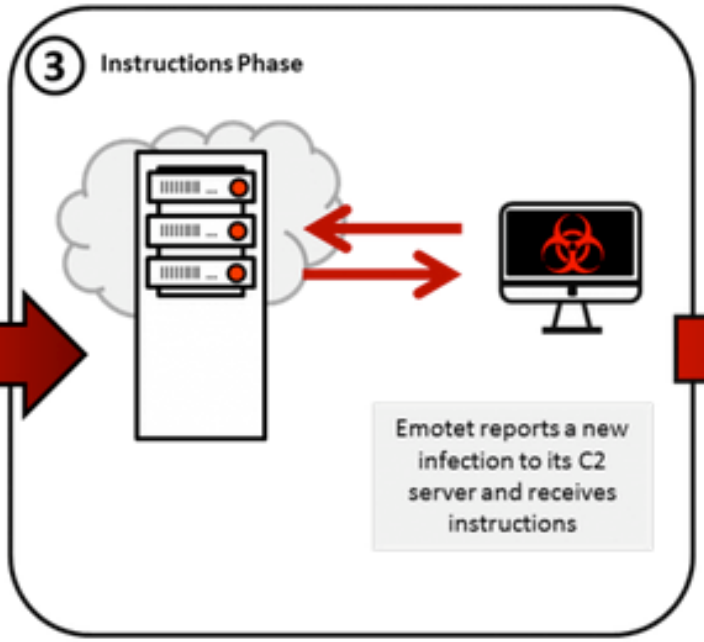


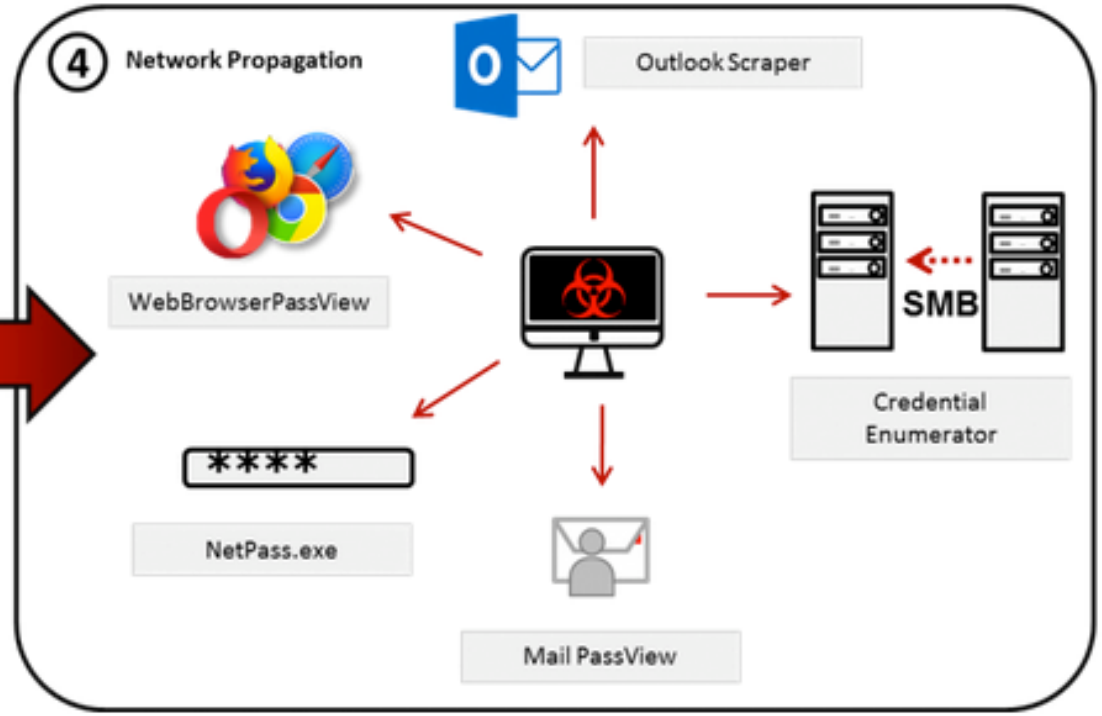
LE MALWARE EMOTET

Concept général d'infection



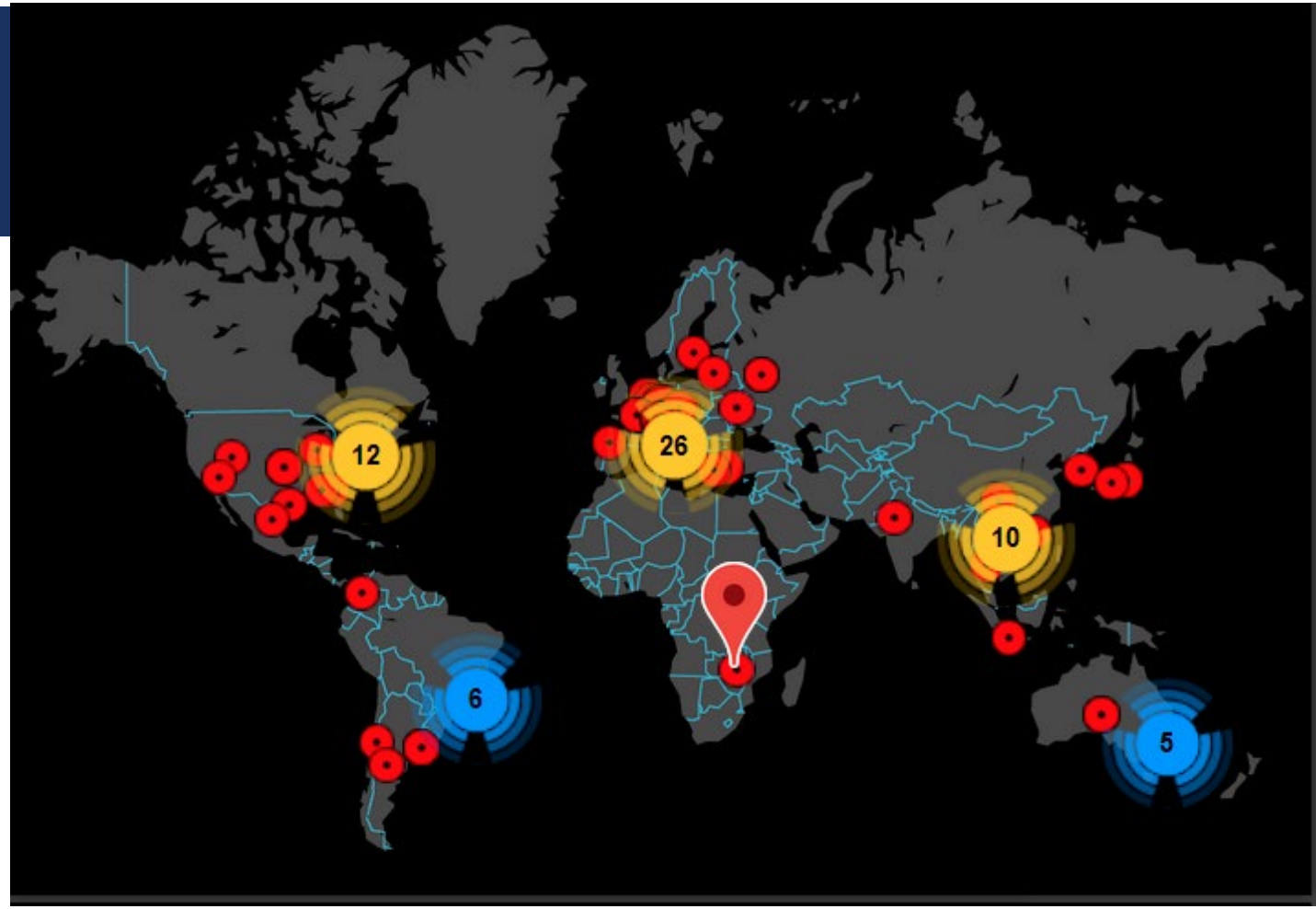


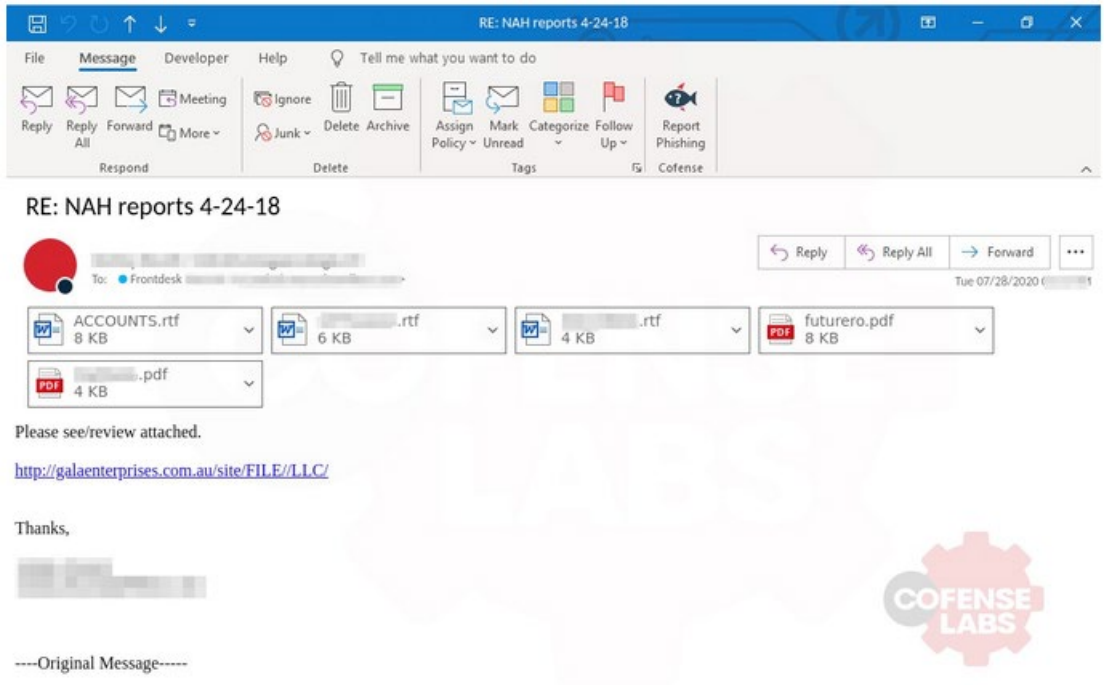




LE MALWARE EMOTET

Retour en force Juillet 2020

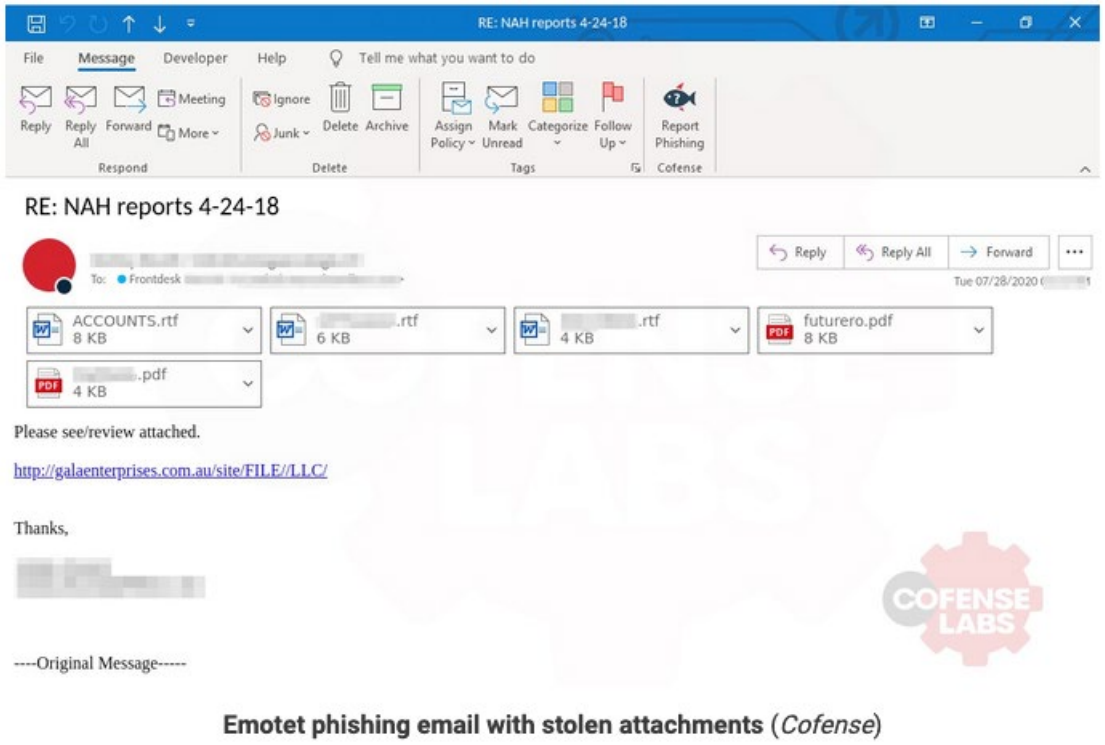




Emotet phishing email with stolen attachments (*Cofense*)

LE MALWARE EMOTET

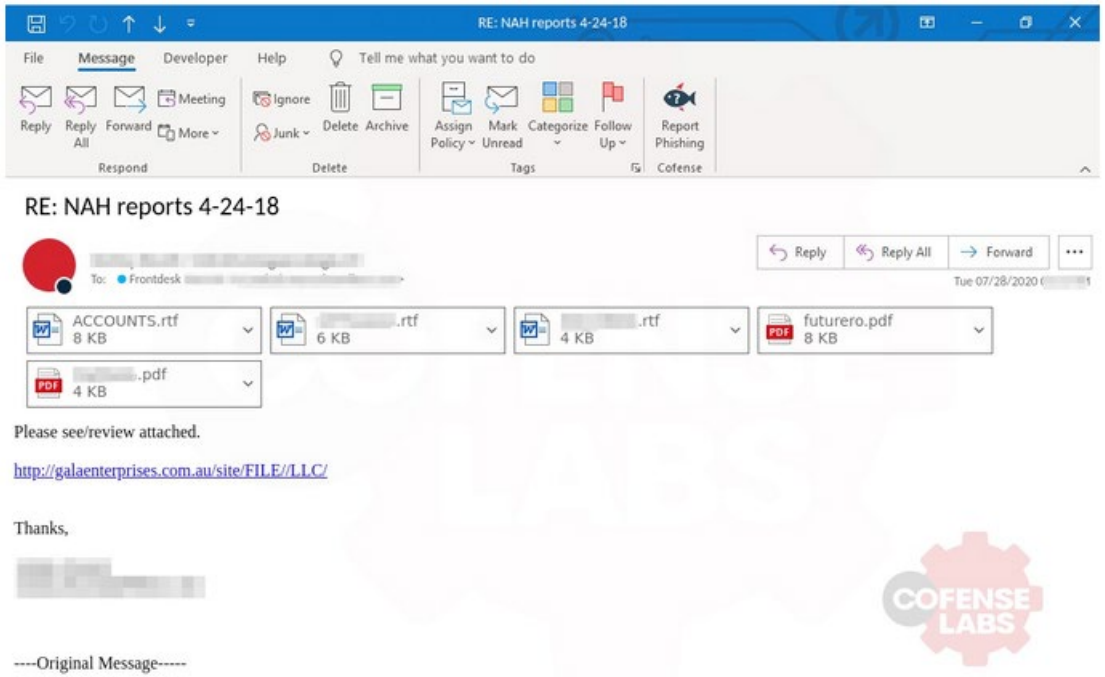
Retour en force Juillet 2020



Emotet phishing email with stolen attachments (*Cofense*)

LE MALWARE EMOTET

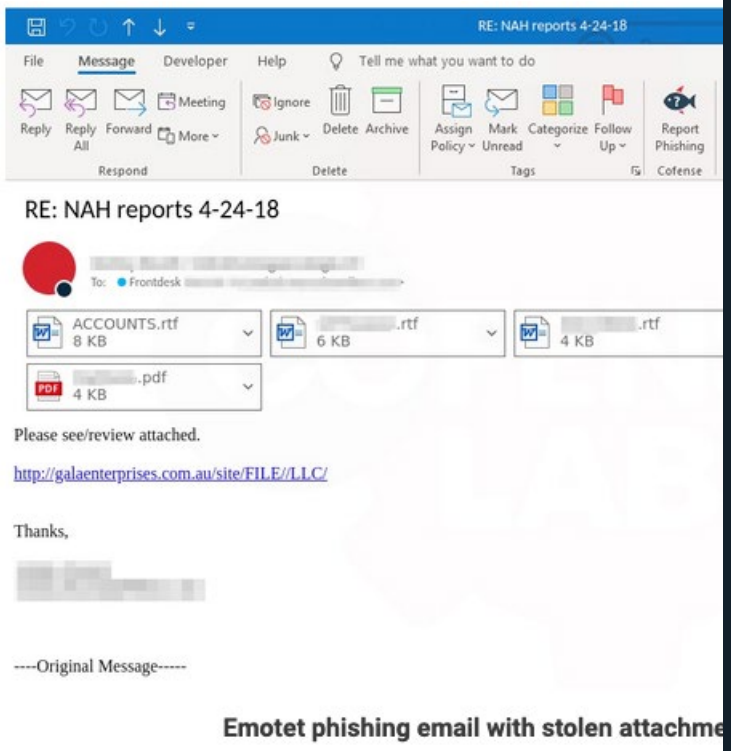
Retour en force Juillet 2020

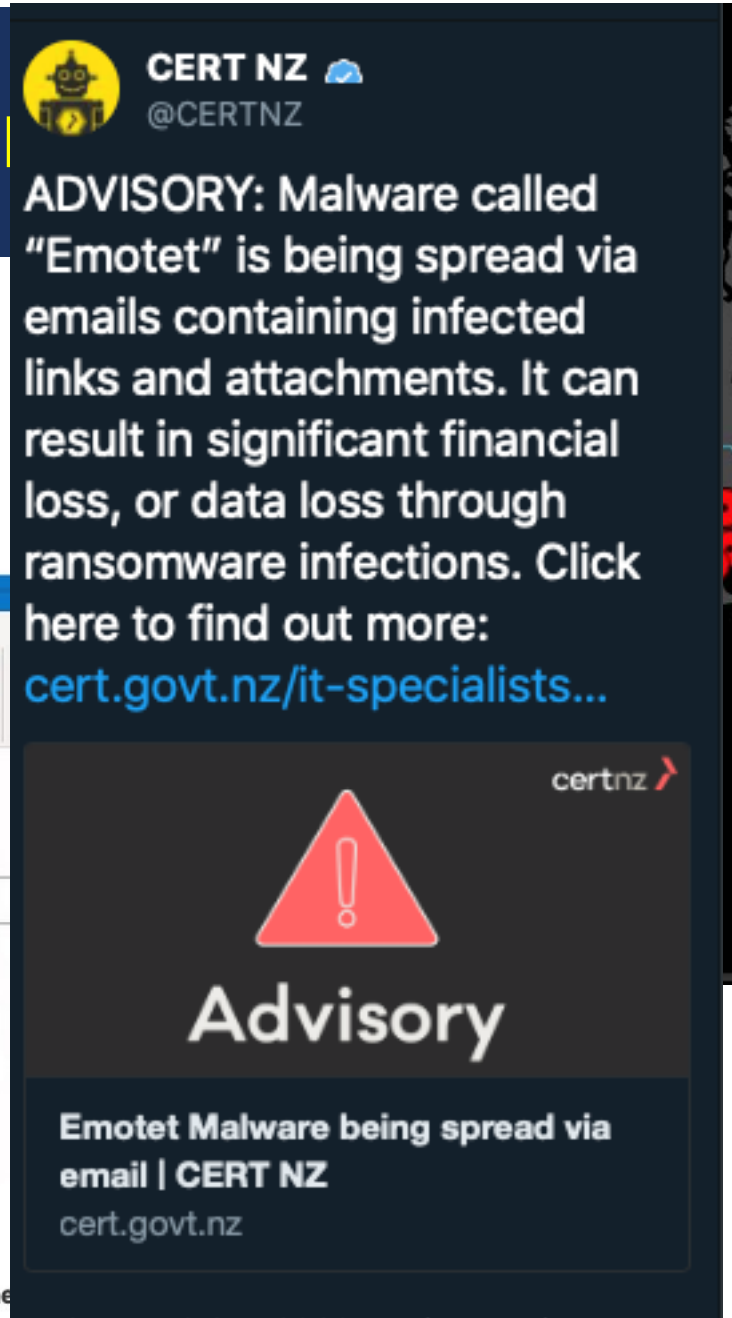


Emotet phishing email with stolen attachments (*Cofense*)

LE MALWARE

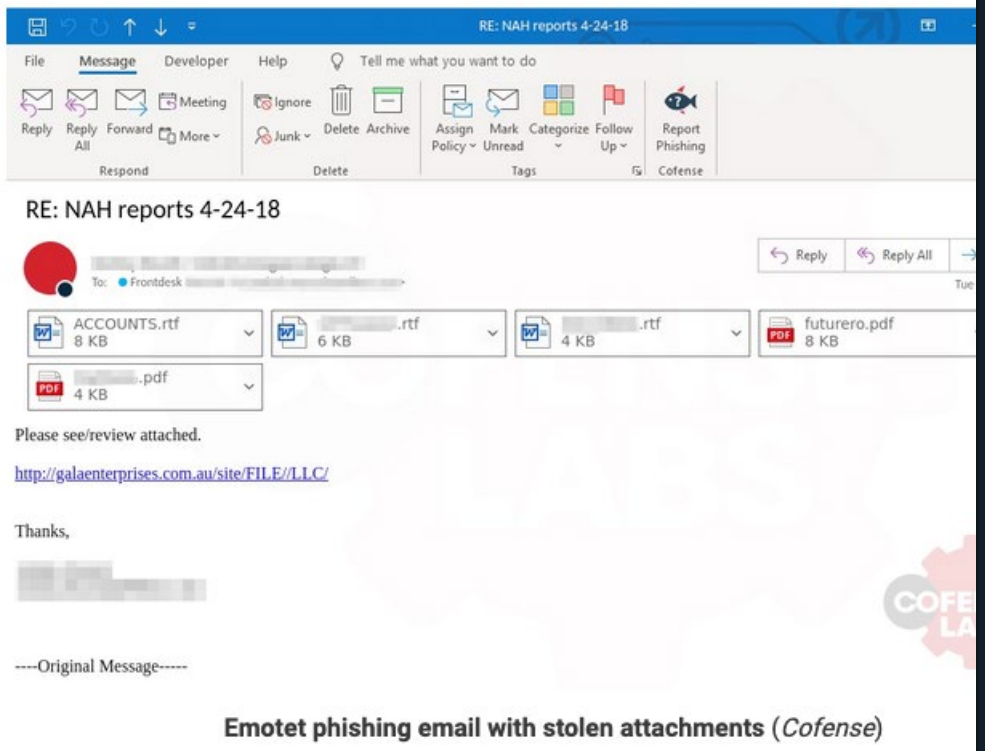
Retour en force Juillet 2020





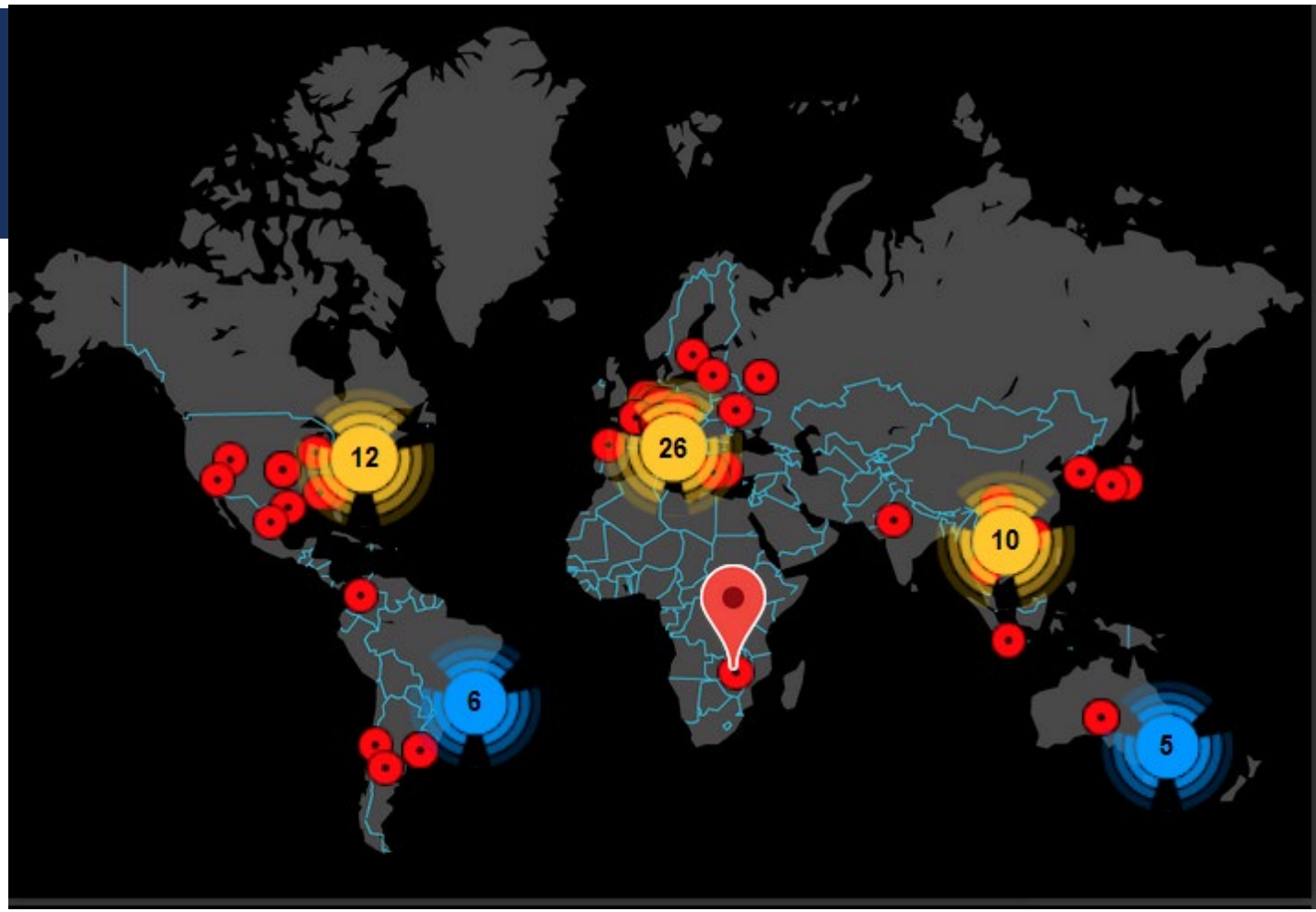
LE MALWARE EMOTET

Retour en force Juillet 2020



Emotet phishing email with stolen attachments (*Cofense*)

EMOTET



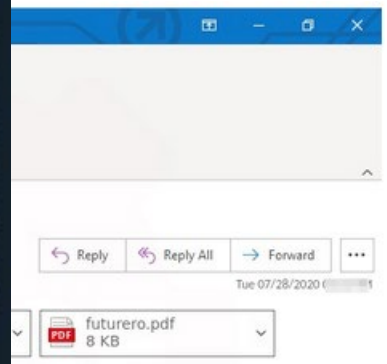
Le Journal de Québec
@JdeQuebec

Des pirates informatiques ont réussi à infiltrer le système du ministère de la Justice (@HugoJoncas) #PolQC #Securité #Enquête #JDQ journaldequebec.com/2020/09/01/le-...

Translate Tweet

Le ministère de la Justice victime de cyberpirates
journaldequebec.com

6:54am · 1 Sep 2020 · Twitter Web App

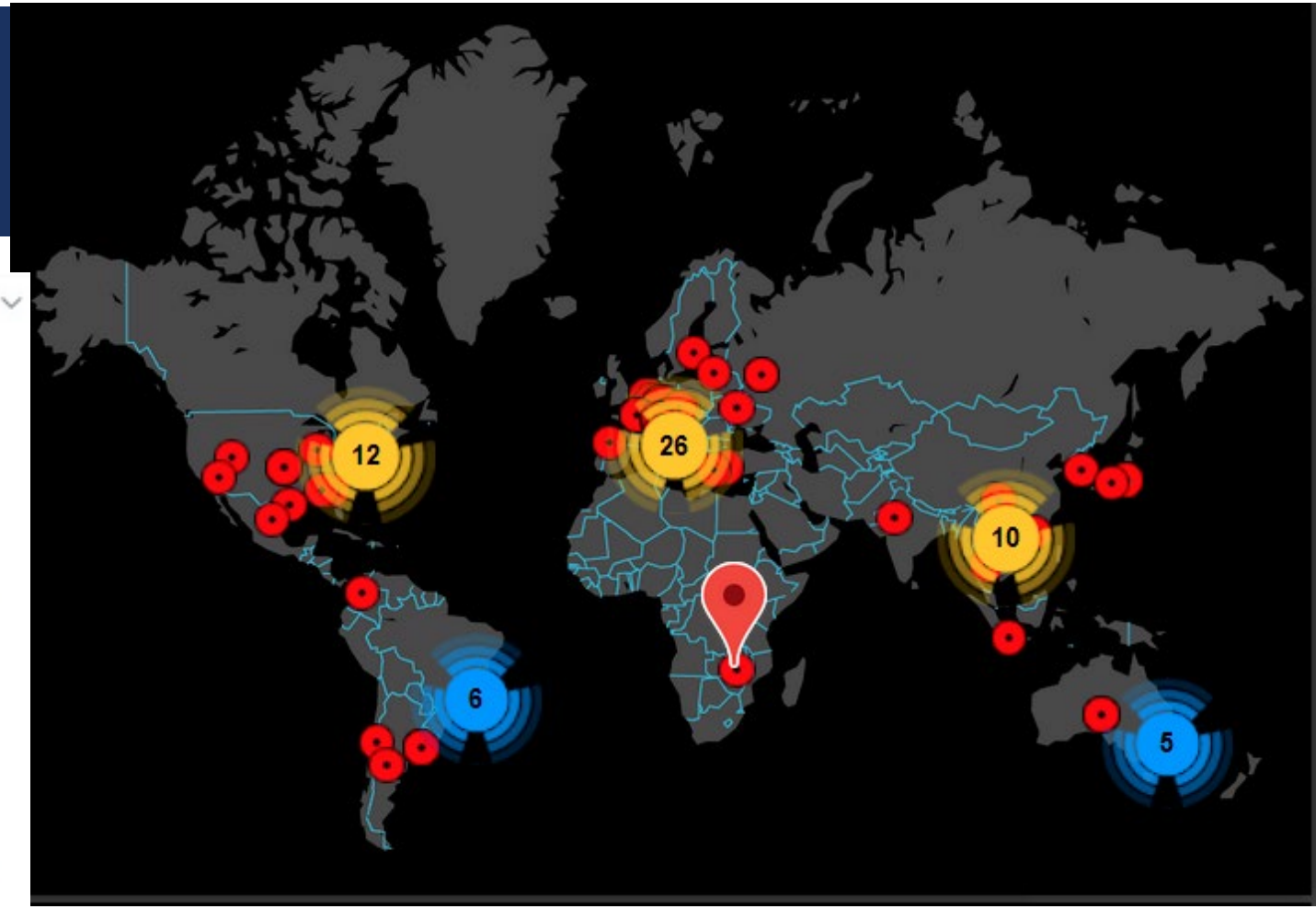


COFENSE LABS

----Original Message-----

Emotet phishing email with stolen attachments (*Cofense*)

LE MALWARE EMOTET



CERT-FR
@CERT_FR

⚠ Alerte CERT-FR ⚠

Depuis quelques jours, l'ANSSI constate un ciblage d'entreprises et administrations françaises par le code malveillant Emotet.

Translated from French by Google

⚠ Alert CERT-FR ⚠

For several days, ANSSI has observed the targeting of French companies and administrations by the malicious code Emotet.

7:46 PM · Sep 7, 2020 · Twitter Web App

----Original Message-----

Emotet phishing email with stolen attachments (*Cofense*)

THE EMOTET MALWARE

THE EMOTET MALWARE

Obdulia Treib

Junk -...fosecsw.ca 11:01

OT

Attn: Hiring Manager - My Job Application

To: info@infosecsw.ca

Dear Hiring Manager:

I was keenly interested in reading the job posting for the position available at your company. I believe my experience is a strong match for the responsibilities pertaining to the roles available, and I'm pleased to submit my application for the position.

I have attached my resume in this letter. Through it, I hope you will learn more about my background, education, achievements, and awards.

If I can provide you with any further information, please let me know. I look forward to hearing from you about this opportunity.

Thank you for your consideration.

myResume.xlsb

THE EMOTET MALWARE

Obdulia Treib

Junk -...fosecsw.ca 11:01

OT

Attn: Hiring Manager - My Job Application

To: info@infosecsw.ca

Dear Hiring Manager:

I was keenly interested in reading the job posting for the position available at your company. I believe my experience is a strong match for the responsibilities pertaining to the roles available, and I'm pleased to submit my application for the position.

I have attached my resume in this letter. Through it, I hope you will learn more about my background, education, achievements, and awards.

If I can provide you with any further information, please let me know. I look forward to hearing from you about this opportunity.

Thank you for your consideration.

myResume.xlsb

VIRUSTOTAL

THE EMOTET MALWARE

Obdulia Treib

Junk -...fosecsw.ca 11:01

OT

Attn: Hiring Manager - My Job Application

To: info@infosecsw.ca

Dear Hiring Manager:

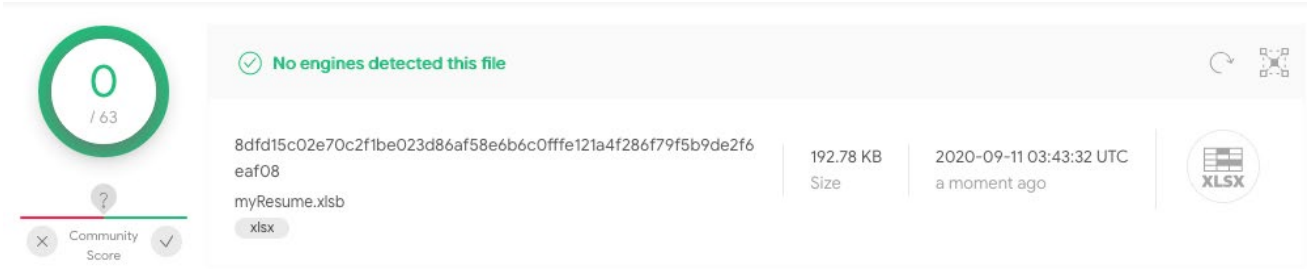
I was keenly interested in reading the job posting for the position available at your company. I believe my experience is a strong match for the responsibilities pertaining to the roles available, and I'm pleased to submit my application for the position.

I have attached my resume in this letter. Through it, I hope you will learn more about my background, education, achievements, and awards.

If I can provide you with any further information, please let me know. I look forward to hearing from you about this opportunity.

Thank you for your consideration.

myResume.xlsb



VIRUSTOTAL

THE EMOTET MALWARE

Obdulia Treib

Junk -...fosecsw.ca 11:01

OT

Attn: Hiring Manager - My Job Application

To: info@infosecsw.ca

Dear Hiring Manager:

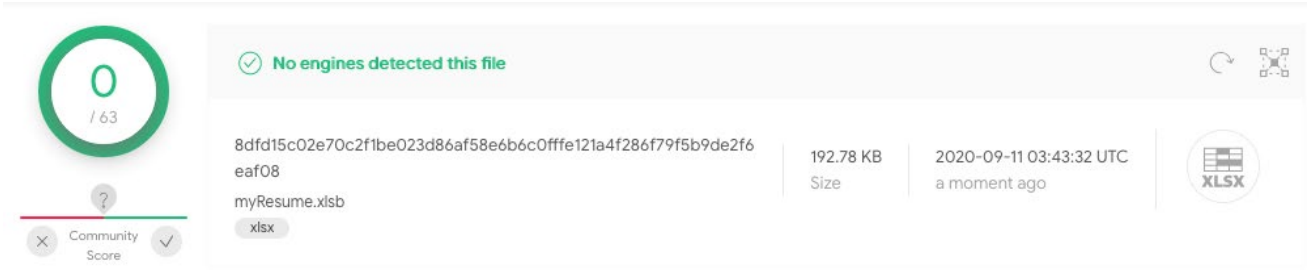
I was keenly interested in reading the job posting for the position available at your company. I believe my experience is a strong match for the responsibilities pertaining to the roles available, and I'm pleased to submit my application for the position.

I have attached my resume in this letter. Through it, I hope you will learn more about my background, education, achievements, and awards.

If I can provide you with any further information, please let me know. I look forward to hearing from you about this opportunity.

Thank you for your consideration.

myResume.xlsb



VIRUSTOTAL

HYBRID ANALYSIS

THE EMOTET MALWARE

Obdulia Treib Junk -...fosecsw.ca 11:01

Attn: Hiring Manager - My Job Application

To: info@infosecsw.ca

Dear Hiring Manager:

I was keenly interested in reading the job posting for the position available at your company. I believe my experience is a strong match for the responsibilities pertaining to the roles available, and I'm pleased to submit my application for the position.

I have attached my resume in this letter. Through it, I hope you will learn more about my background, education, achievements, and awards.

If I can provide you with any further information, please let me know. I look forward to hearing from you about this opportunity.

Thank you for your consideration.

myResume.xlsb

Submission name:	myResume.xlsb
Size:	193KiB
Type:	xlsx office
Mime:	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
SHA256:	8dfd15c02e70c2f1be023d86af58e6b6c0fffe121a4f286f79f5b9de2f6eaf08
Last Anti-Virus Scan:	09/11/2020 03:46:05 (UTC)
Last Sandbox Report:	09/11/2020 03:45:33 (UTC)

suspicious

AV Detection: 1%

Link Twitter E-Mail

Anti-Virus Results

Refresh

CrowdStrike Falcon

CLEAN

Static Analysis and ML

Last Update: 09/11/2020 03:46:05 (UTC)

View Details: N/A

Visit Vendor:

GET STARTED WITH A FREE TRIAL

MetaDefender

3%

Multi Scan Analysis

Last Update: 09/11/2020 03:46:05 (UTC)

View Details:

Visit Vendor:

VirusTotal

CLEAN

Multi Scan Analysis

Last Update: 09/11/2020 03:46:05 (UTC)

View Details:

Visit Vendor:

HYBRID ANALYSIS

0 / 63

Community Score

No engines detected this file

8dfd15c02e70c2f1be023d86af58e6b6c0fffe121a4f286f79f5b9de2f6eaf08

myResume.xlsb

xlsx

192.78 KB Size

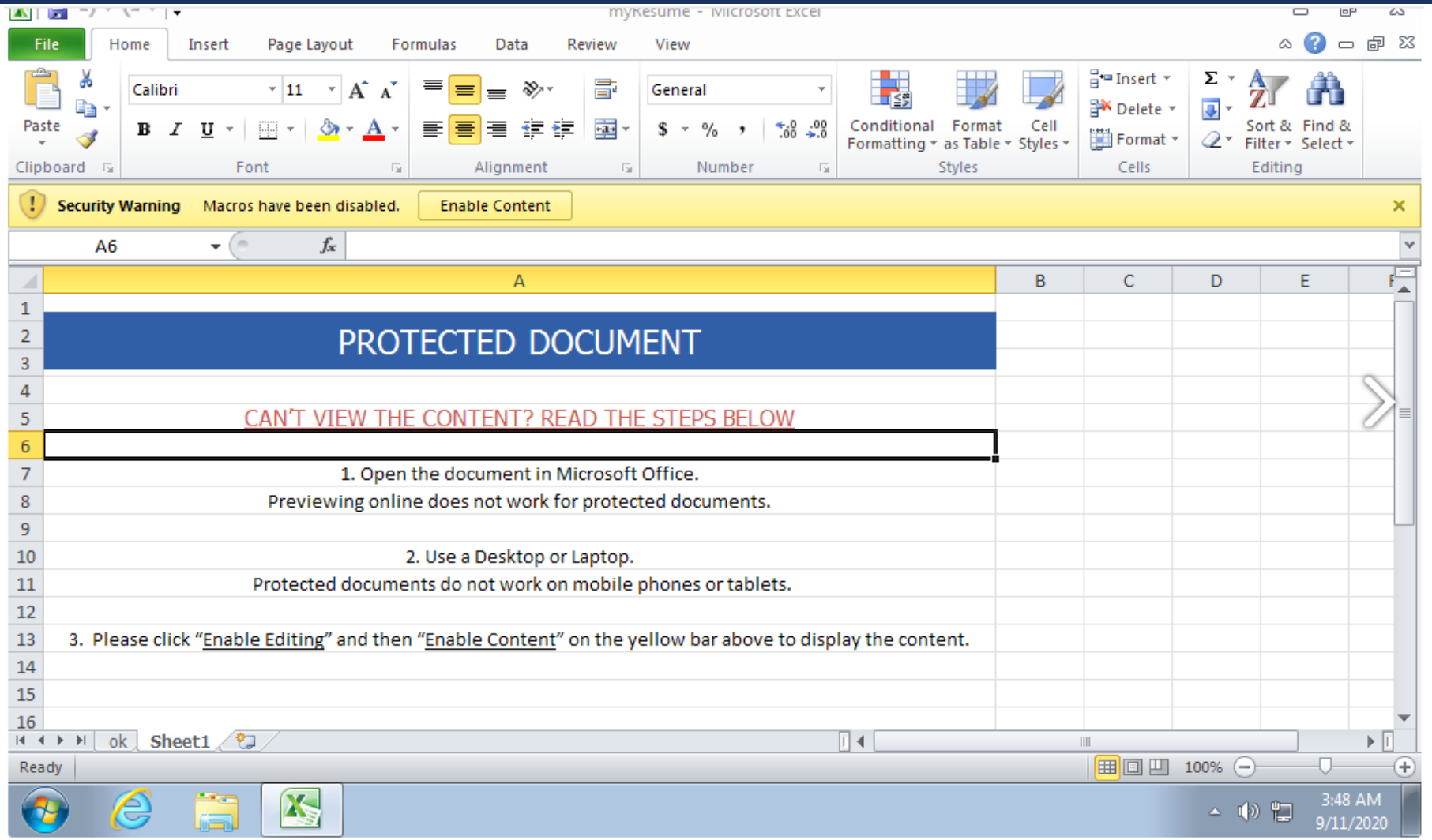
2020-09-11 03:43:32 UTC a moment ago

XLSX

VIRUSTOTAL

THE EMOTET MALWARE

THE EMOTET MALWARE



THE EMOTET MALWARE

THE EMOTET MALWARE

THE EMOTET MALWARE

Malicious Indicators

Network Related

Malicious artifacts seen in the context of a contacted host

details Found malicious artifacts related to "205.185.125.104": ...

URL: http://205.185.125.104/files/june23.dll (AV positives: 16/79 scanned on 09/10/2020 15:17:07)
URL: http://205.185.125.104/files/tor.exe (AV positives: 16/79 scanned on 09/10/2020 03:01:38)
URL: http://205.185.125.104/files/812.db (AV positives: 16/79 scanned on 09/09/2020 23:06:00)
URL: http://205.185.125.104/ (AV positives: 8/79 scanned on 09/09/2020 13:01:56)
URL: http://205.185.125.104/files/july27.dll (AV positives: 17/79 scanned on 09/08/2020 03:19:50)
File SHA256: 90d088ada7c60c82a5881cc3dd095d8ede8b2086b4ed89fdb38872105e3c5bb4 (AV positives: 37/74 scanned on 08/17/2020 11:26:26)
File SHA256: 02846dbf25b333625a0720075fb47da62a946e5b0b4f9e9ba14cef514d576b37 (AV positives: 37/75 scanned on 07/29/2020 10:22:44)
File SHA256: acdf04f8a8ea20b485aaa4f8f30b4be075775d5599b3006bbc020aba2a5d40b7 (AV positives: 2/75 scanned on 07/28/2020 18:46:34)
File SHA256: c1532b3d37ff2ec7d70d7f8037b8cdf843d3cdd24adf860f4251d045ddf9d47c (AV positives: 39/75 scanned on 07/27/2020 12:28:08)
File SHA256: a5ec2f495c117f199e1cecc1e2c9e5ad7f4f8241eb0784bb82da89c5ac88778b (AV positives: 22/75 scanned on 07/23/2020 21:02:44)
File SHA256: 33ce28d0b499f2d15f3cccb5979367cffe7fd8202282e255c95b7a62fa44569f (Date: 07/13/2020 19:11:47)

source Network Traffic

relevance 10/10

THE EMOTET MALWARE

Malicious Indicators

Network Related

Malicious artifacts seen in the context of a contacted host

details Found malicious artifacts related to "205.185.125.104": ...

URL: http://205.185.125.104/files/june23.dll (AV positives: 16/79 scanned on 09/10/2020 15:17:07)
URL: http://205.185.125.104/files/tor.exe (AV positives: 16/79 scanned on 09/10/2020 03:01:38)
URL: http://205.185.125.104/files/812.db (AV positives: 16/79 scanned on 09/09/2020 23:06:00)
URL: http://205.185.125.104/ (AV positives: 8/79 scanned on 09/09/2020 13:01:56)
URL: http://205.185.125.104/files/july27.dll (AV positives: 17/79 scanned on 09/08/2020 03:19:50)
File SHA256: 90d088ada7c60c82a5881cc3dd095d8ede8b2086b4ed89fdb38872105e3c5bb4 (AV positives: 37/74 scanned on 08/17/2020 11:26:26)
File SHA256: 02846dbf25b333625a0720075fb47da62a946e5b0b4f9e9ba14cef514d576b37 (AV positives: 37/75 scanned on 07/29/2020 10:22:44)
File SHA256: acdf04f8a8ea20b485aaa4f8f30b4be075775d5599b3006bbc020aba2a5d40b7 (AV positives: 2/75 scanned on 07/28/2020 18:46:34)
File SHA256: c1532b3d37ff2ec7d70d7f8037b8cdf843d3cdd24adf860f4251d045ddf9d47c (AV positives: 39/75 scanned on 07/27/2020 12:28:08)
File SHA256: a5ec2f495c117f199e1cecc1e2c9e5ad7f4f8241eb0784bb82da89c5ac88778b (AV positives: 22/75 scanned on 07/23/2020 21:02:44)
File SHA256: 33ce28d0b499f2d15f3cccb5979367cffe7fd8202282e255c95b7a62fa44569f (Date: 07/13/2020 19:11:47)

source Network Traffic

relevance 10/10

MALICIOUS

myResume.xlsb

Analyzed on: 09/11/2020 03:45:45 (UTC)

Environment: Windows 7 64 bit

Threat Score: 62/100

AV Detection: Marked as clean

Indicators: 1 2 11

Network:

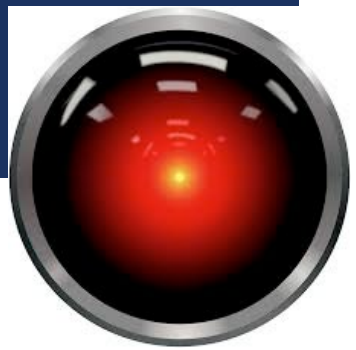
HYBRID ANALYSIS

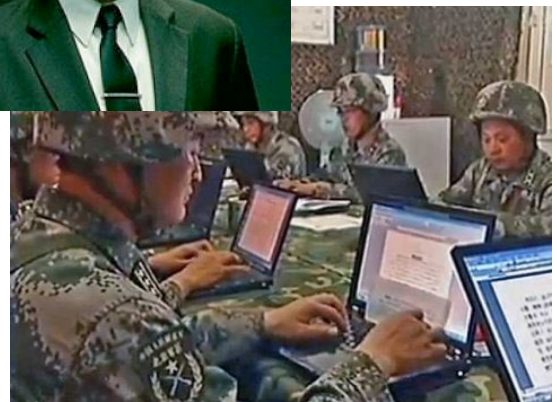
REFLEXION …

Which one will be the most effective to protect us from our future

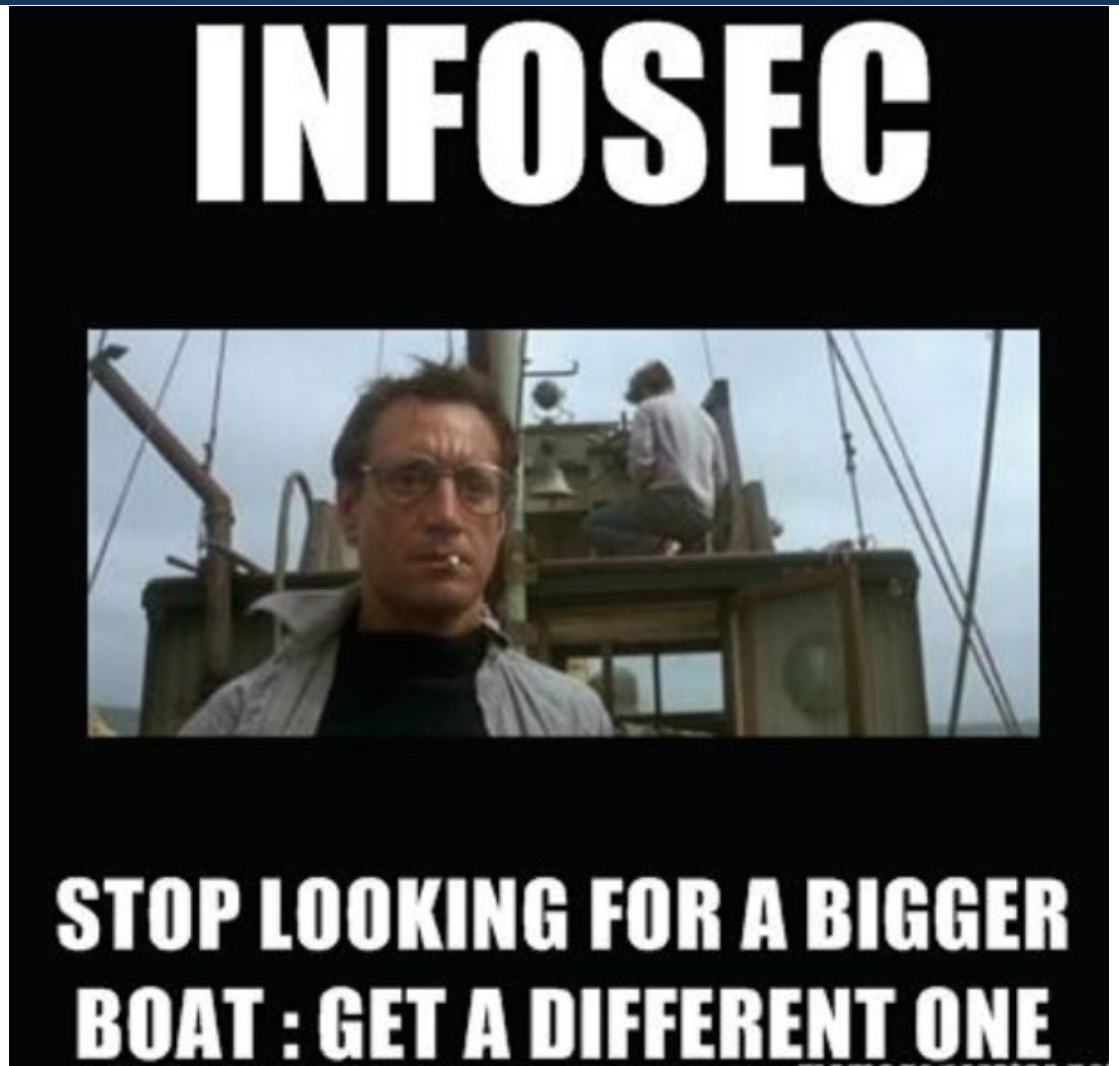
DIFFÉRENTS TYPES DE PIRATES INFORMATIQUE

KNOW YOUR ENEMY





REFLEXION …



LES MAUDITS MOTS DE PASSE

LA SÉCURITÉ EST AUSSI FORTE QUE SON MAILLON LE PLUS FAIBLE

BAD PRACTICE

https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

BAD PRACTICE

#1 password in 2016 ==========➔

https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

BAD PRACTICE

#1 password in 2016 ==========➔

KEEPER

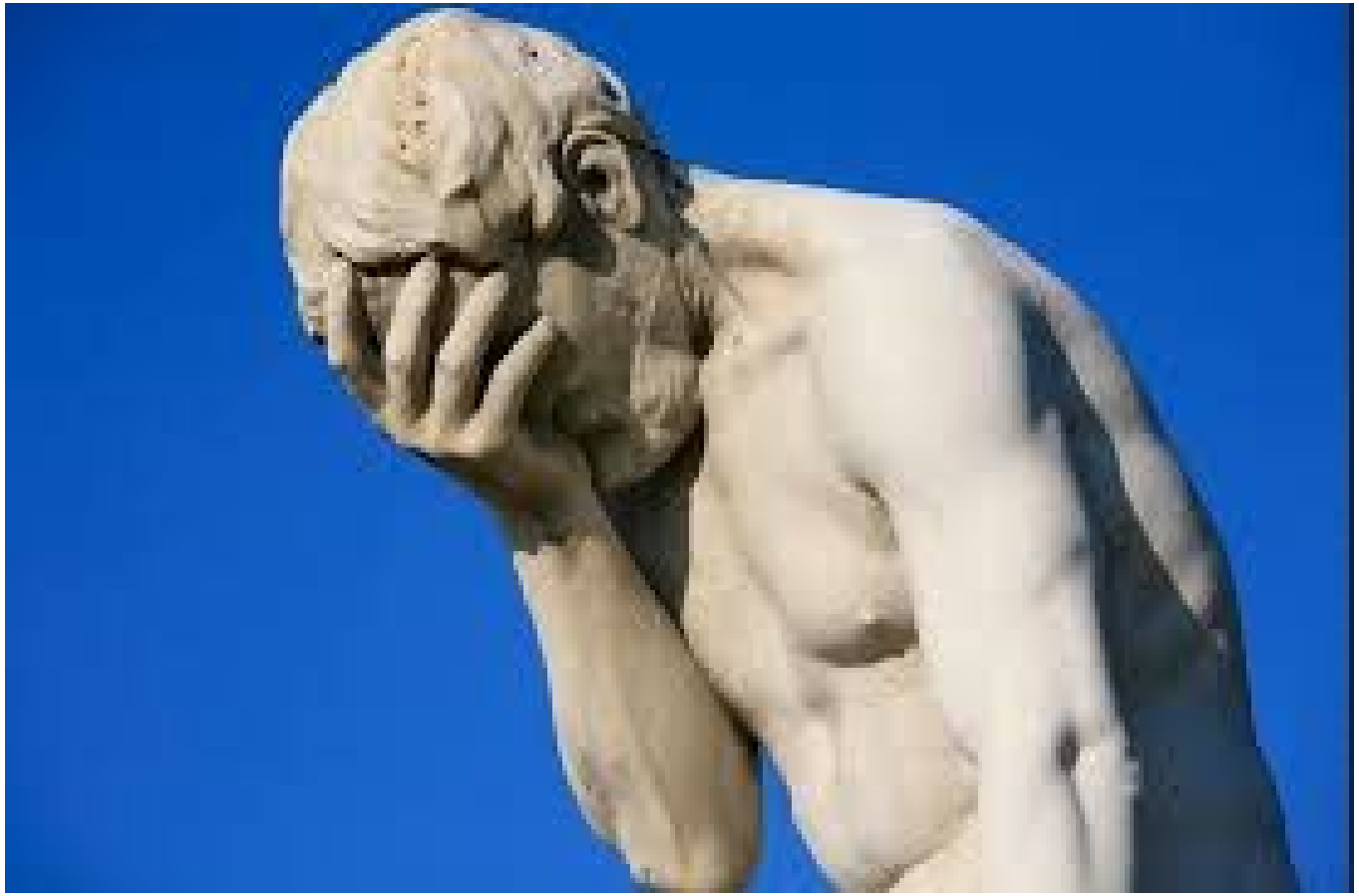
https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321
11.	qwertyuiop
12.	mynoob
13.	123321
14.	666666
15.	18atcskd2w

BAD PRACTICE

#1 password in 2016 ==========➔



KEEPER

https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321
11.	qwertyuiop
12.	mynoob
13.	123321
14.	666666
15.	18atcskd2w

BAD EXAMPLE

https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14

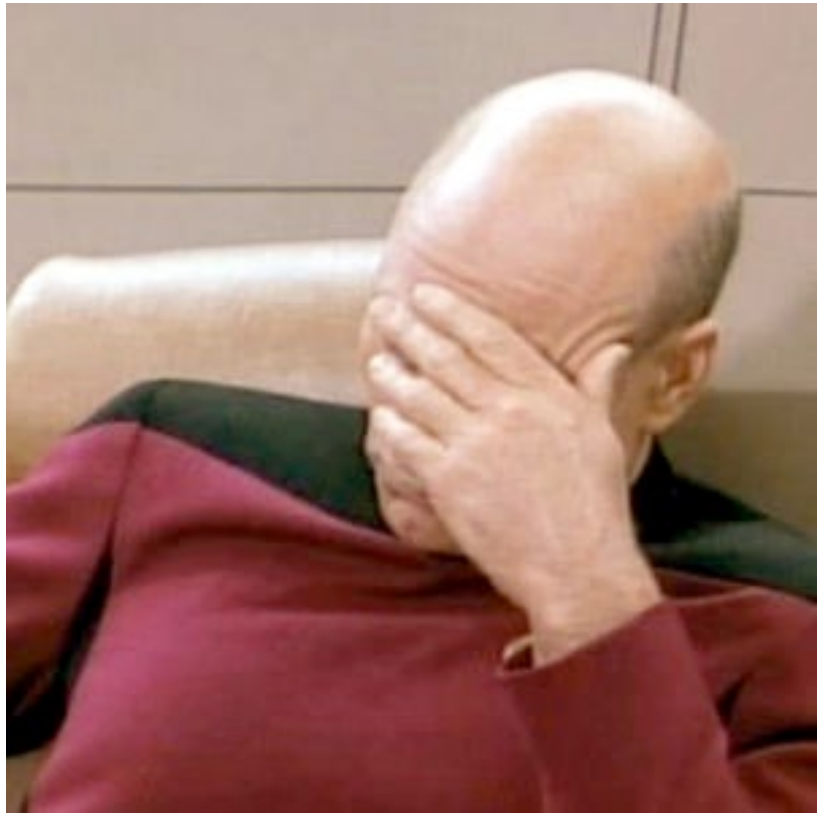
BAD EXAMPLE

From a collection of 463,619,984 MP

https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14

BAD EXAMPLE

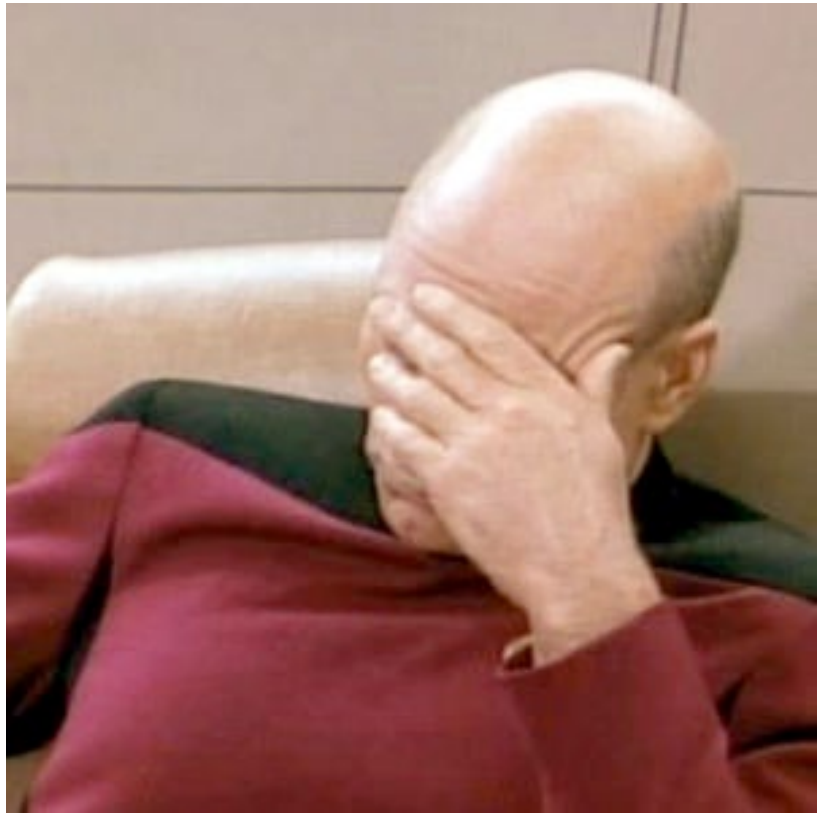
From a collection of 463,619,984 MP



https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14

BAD EXAMPLE

From a collection of 463,619,984 MP

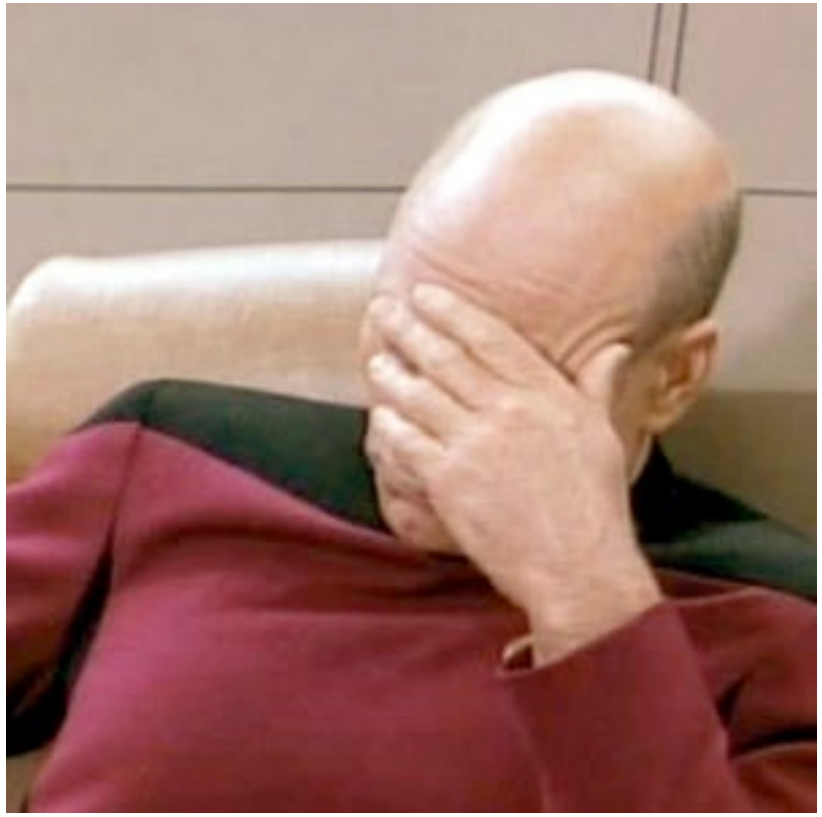


1	9218720	123456
2	3103503	123456789
3	1651385	qwerty
4	1313464	password
5	1273179	111111
6	1126222	12345678
7	1085144	abc123
8	969909	1234567
9	952446	password1
10	879924	1234567890
11	866640	123123
12	834468	12345
13	621078	homelesspa
14	564344	iloveyou
15	527158	1q2w3e4r5t

https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14

BAD EXAMPLE

From a collection of 463,619,984 MP



#1 password in 2017

1	9218720	123456
2	3103503	123456789
3	1651385	qwerty
4	1313464	password
5	1273179	111111
6	1126222	12345678
7	1085144	abc123
8	969909	1234567
9	952446	password1
10	879924	1234567890
11	866640	123123
12	834468	12345
13	621078	homelesspa
14	564344	iloveyou
15	527158	1q2w3e4r5t

4iQ

https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14

INCREDIBLE……

Source: https://www.teamsid.com/100-worst-passwords-top-50/

INCREDIBLE……

Documented by

Source: https://www.teamsid.com/100-worst-passwords-top-50/

INCREDIBLE…….

Documented by 

Source: https://www.teamsid.com/100-worst-passwords-top-50/

INCREDIBLE…….

Documented by splashdata

Source: https://www.teamsid.com/100-worst-passwords-top-50/

INCREDIBLE……

Documented by splashdata

Source: https://www.teamsid.com/100-worst-passwords-top-50/

Rang	Mots de passe
#20	!@#$%^&*
#19	654321
#18	monkey
#17	123123
#16	football
#15	abc123
#14	666666
#13	welcome
#12	admin
#11	princess
#10	iloveyou
#9	qwerty
#8	sunshine
#7	1234567
#6	111111
#5	12345
#4	12345678
#3	123456789
#2	password
#1	123456

INCREDIBLE……

Documented by splashdata

Source: https://www.teamsid.com/100-worst-passwords-top-50/

Rang	Mots de passe
#20	!@#$%^&*
#19	654321
#18	monkey
#17	123123
#16	football
#15	abc123
#14	666666
#13	welcome
#12	admin
#11	princess
#10	iloveyou
#9	qwerty
#8	sunshine
#7	1234567
#6	111111
#5	12345
#4	12345678
#3	123456789
#2	password
#1	123456

MY HAIR IS FALLING OFF

Documented by

Source: https://www.teamsid.com/100-worst-passwords-top-50/

MY HAIR IS FALLING OFF

Documented by 

Source: https://www.teamsid.com/100-worst-passwords-top-50/

MY HAIR IS FALLING OFF

Documented by splashdata

Source: https://www.teamsid.com/100-worst-passwords-top-50/

MY HAIR IS FALLING OFF

Documented by splashdata

Source: https://www.teamsid.com/100-worst-passwords-top-50/

Rang	Mots de passe
#20	888888
#19	7777777
#18	lovely
#17	555555
#16	654321
#15	qwertyuiop
#14	admin
#13	1q2w3e4r
#12	qwerty123
#11	abc123
#10	123123
#9	111111
#8	iloveyou
#7	12345
#6	12345678
#5	1234567
#4	password
#3	qwerty
#2	123456789
#1	123456

MY HAIR IS FALLING OFF

Documented by splashdata

Rang	Mots de passe
#20	888888
#19	7777777
#18	lovely
#17	555555
#16	654321
#15	qwertyuiop
#14	admin
#13	1q2w3e4r
#12	qwerty123
#11	abc123
#10	123123
#9	111111
#8	iloveyou
#7	12345
#6	12345678
#5	1234567
#4	password
#3	qwerty
#2	123456789
#1	123456

AGAIN in #1 2019

Source: https://www.teamsid.com/100-worst-passwords-top-50/

2020 - OMG

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

Source: https://nordpass.com/most-common-passwords-list/

2020 - OMG

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

UNREAL #1 2020

Source: https://nordpass.com/most-common-passwords-list/

CLASSIFICATION DE L'INFORMATION

Exemple de classification de l'information au GC

Renseignements et biens de nature délicate du gouvernement

Protégé

Lorsque l'on peut raisonnablement s'attendre à ce qu'une divulgation non autorisée porte atteinte à un intérêt autre que l'intérêt national, c'est à-dire à l'intérêt d'une personne ou d'une organisation.

Protégé A
Préjudice à une personne, une organisation ou un gouvernement.

Protégé B
Préjudice grave à une personne, une organisation ou un gouvernement.

Protégé C
Préjudice extrêmement grave à une personne, une organisation ou un gouvernement.

Classifié

Lorsque l'on peut raisonnablement s'attendre à ce qu'une divulgation non autorisée porte atteinte à l'intérêt national, c'est à-dire à la défense et au maintien de la stabilité sociopolitique et économique du Canada.

Confidentiel
Préjudice à l'intérêt national.

Secret
Préjudice grave à l'intérêt national.

Très secret
Préjudice extrêmement grave à l'intérêt national.

Personnel

Cote de fiabilité

Exigée d'un employé qui travaille sur un contrat fédéral de nature délicate pour accéder aux renseignements et aux biens Protégés (A, B ou C).

Attestation de sécurité sur le personnel

Exigée d'un employé qui travaille sur un contrat fédéral de nature délicate pour accéder aux renseignements et aux biens Classifiés (confidentiel, secret, très secret) (peux aussi accéder aux renseignements et aux biens Protégés).

Organisation du secteur privé

Vérification d'organisation désignée (VOD)

Permet à une entreprise d'envoyer des employés avec un besoin de connaître et qui ont fait l'objet d'une enquête de sécurité appropriée sur des lieux de travail à accès réglementé et de leur donner accès à des renseignements et à des biens Protégés.

Attestation de sécurité d'installation (ASI)

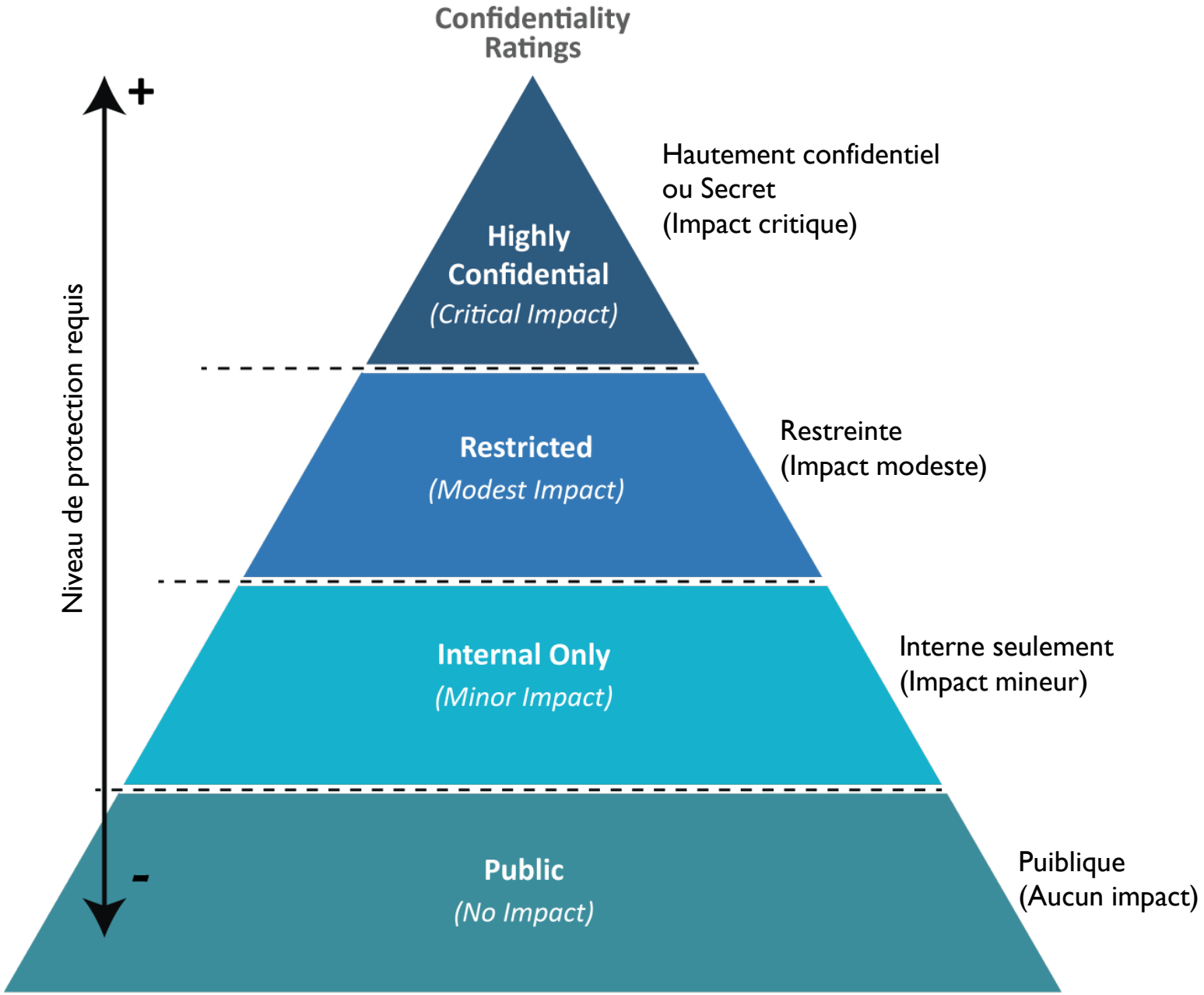
Permet à une entreprise d'envoyer des employés avec un besoin de connaître et qui ont fait l'objet d'une enquête de sécurité appropriée sur des lieux de travail à accès réglementé et de leur donner accès à des renseignements et à des biens Protégés et Classifiés.

Organisation du Traité de l'Atlantique Nord (OTAN) : Les niveaux de sécurité classifiés du Canada correspondent à ceux de l'OTAN, mais nécessitent une séance d'information spéciale et un engagement à respecter les exigences applicables de l'OTAN.

Des attestations de sécurité supplémentaires peuvent être accordées aux organisations qui font l'objet d'une VOD ou d'une ASI.

Autorisation de détenir des renseignements (ADR) : autorisation de détenir, de traiter et de protéger des renseignements ou des biens Protégés ou Classifiés sur les lieux de travail. **Production :** autorisation de produire des biens de nature délicate. **Sécurité physique liée à la sécurité des TI et COMSEC/INFOSEC :** peut être un critère dans certains contrats.

Niveaux de classification généraux



SOLUTIONS ÉDUCATIVES

EMPLOI EN SECINFO
PERSPECTIVES DE PLACEMENT

PARTOUT !

LE SAVOIR

NOVIPRO

La protection ultime viens de l'éducation et la formation

Les conférences

- → Haiti CyberCon
- → HackFest – Québec 16-21 nov. 2020
- → **NOVIPRO 2020** ←

- Les formations de sensibilisations
  - Séminaire de Sherbrooke

- Formation universitaire (Canada)
  - **U de Sherbrooke** (CefTI)
    - Micro-programme 2e cycle en cybersécurité
  - Ecole Polytechnique de Montréal
    - Programme de 3 certificats
  - Concordia University (2020)
- Secteur privée

  Centres de formation privés

FORMATION UNIVERSITAIRE D'APPOINT

UNIVERSITÉ DE SHERBROOKE

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet prévention

Objectif(s) général(aux)

Permettre à l'étudiante ou à l'étudiant de :

- maîtriser les tenants et aboutissants de la sécurité informatique contemporaine;
- maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI;
- savoir concevoir, mettre en œuvre et documenter une stratégie efficace pour protéger et défendre ces surfaces d'attaque, en tenant compte d'un budget de ressources donné;
- pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses.

https://www.usherbrooke.ca/admission/programme/47V/microprogramme-de-2e-cycle-en-securite-informatique-volet-prevention/

FORMATION UNIVERSITAIRE D'APPOINT

UNIVERSITÉ DE SHERBROOKE

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet prévention

Activités pédagogiques obligatoires

Code de l'activité pédagogique	Titre de l'activité pédagogique et nombre de crédits
INF801	Concepts de base de la sécurité en TI - 3 crédits
INF802	Planification et prévention en sécurité TI - 3 crédits
INF803	Sécurité des systèmes - 3 crédits
INF810	Projet en sécurité 1 - 3 crédits

https://www.usherbrooke.ca/admission/programme/47V/microprogramme-de-2e-cycle-en-securite-informatique-volet-prevention/

FORMATION UNIVERSITAIRE D'APPOINT

UNIVERSITÉ DE SHERBROOKE

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet prévention

Activités pédagogiques à option - à 3 crédits

Une activité pédagogique choisie parmi les suivantes :

Code de l'activité pédagogique	Titre de l'activité pédagogique et nombre de crédits
INF804	Sécurité des logiciels - 3 crédits
INF806	Système et réseau - 3 crédits
INF809	Architecture de sécurité - 3 crédits

https://www.usherbrooke.ca/admission/programme/47V/microprogramme-de-2e-cycle-en-securite-informatique-volet-prevention/

FORMATION UNIVERSITAIRE D'APPOINT

UNIVERSITÉ DE SHERBROOKE

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet réaction

Objectif(s) général(aux)
Permettre à l'étudiante ou à l'étudiant de :

- maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure;
- savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale;
- savoir dresser et exécuter un plan d'intervention en cas d'incident et de brèche de données, de manière à trouver le meilleur compromis entre la minimisation des dommages et l'interruption des activités de l'organisation.

https://www.usherbrooke.ca/admission/programme/47W/microprogramme-de-2e-cycle-en-securite-informatique-volet-reaction/

FORMATION UNIVERSITAIRE D'APPOINT

UNIVERSITÉ DE SHERBROOKE

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet réaction

Activités pédagogiques obligatoires

Code de l'activité pédagogique	Titre de l'activité pédagogique et nombre de crédits
INF805	Introduction aux attaques informatiques - 3 crédits
INF807	Criminalistique en sécurité TI - 3 crédits
INF808	Réaction aux attaques et analyses des attaques - 3 crédits
INF811	Projet en sécurité 2 - 3 crédits

https://www.usherbrooke.ca/admission/programme/47W/microprogramme-de-2e-cycle-en-securite-informatique-volet-reaction/

FORMATION UNIVERSITAIRE D'APPOINT

UNIVERSITÉ DE SHERBROOKE

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet réaction

Activités pédagogiques à option - à 3 crédits

Une activité pédagogique choisie parmi les suivantes :

Code de l'activité pédagogique	Titre de l'activité pédagogique et nombre de crédits
INF804	Sécurité des logiciels - 3 crédits
INF806	Système et réseau - 3 crédits
INF809	Architecture de sécurité - 3 crédits

https://www.usherbrooke.ca/admission/programme/47W/microprogramme-de-2e-cycle-en-securite-informatique-volet-reaction/

FORMATION UNIVERSITAIRE DE CHOIX

PRIMEUR : Janvier 2021 –

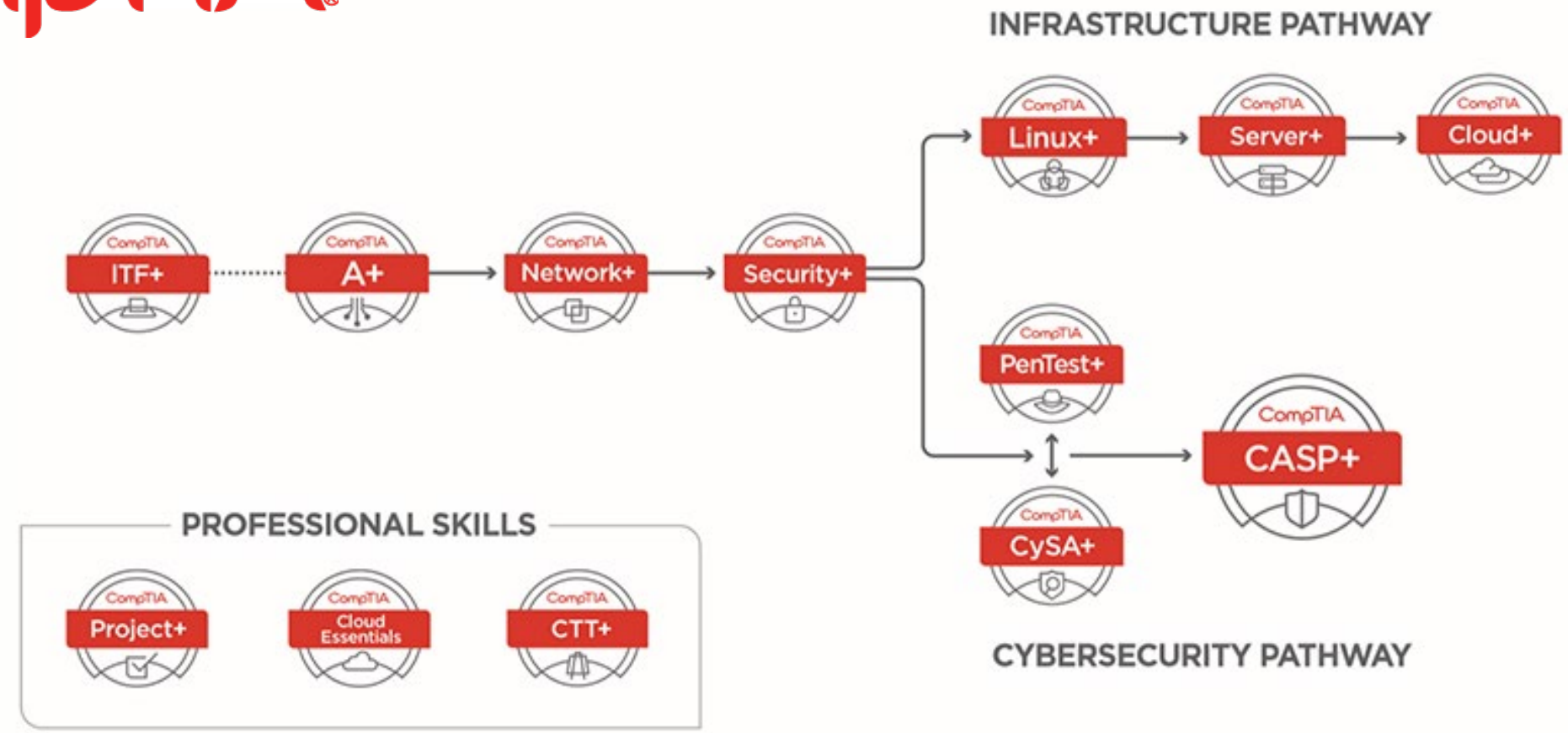
Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Ce diplôme inclut les deux microprogrammes existants en sécurité.

CERETIFIER SON SAVOIR

CERETIFIER SON SAVOIR

CompTIA



PERSPECTIVES DE PLACEMENT

Une ou un spécialiste en cyberdéfense

Les spécialistes en cyberdéfense seront appelés à travailler dans un ou plusieurs services de cyberdéfense offerts par le Centre gouvernemental de cyberdéfense ainsi que ses Centres opérationnels

Conditions salariales
À titre indicatif, l'échelle salariale est de :
45 219 $ (minimum de l'échelle) à
84 908 $ (maximum de l'échelle) en date du 31 mars 2020.

PERSPECTIVES DE PLACEMENT

CONSEILLÈRE OU CONSEILLER EN SÉCURITÉ DE L'INFORMATION

Les salaires varient de 83 250,00 $ à 105 060,00 $, selon le niveau

Qualifications constituant un atout ?

Vous devez clairement démontrer dans votre demande que vous possédez les expertises spécialisées suivants, s'ils s'appliquent à vous, puisqu'ils serviront à déterminer quelle équipe du CST correspond le mieux à votre profil.

Expertises spécialisées

- Virtualisation de réseaux, technologies en nuage et/ou cryptographie.
- Gestion des identités et de l'accès.
- Rédaction ou utilisation des évaluations des menaces et des risques.
- Mise à l'essai et évaluation de produits.
- Gestion de système lié à la sécurité de serveurs Windows ou Linux ou de poste de travail (ce qui comprend les machines virtuelles).
- Configuration de sécurité des plateformes de télécommunications ou de communications unifiées d'entreprise et/ou du réseautage d'entreprise (p. ex., Cisco ou Juniper).
- Utilisation des protocoles de sécurité (p. ex., TLS, HTTPS, IPSec et IKE), des protocoles de communication (p. ex., VoIP/SIP, interfaces REST, RCP et diffusion TCP) et/ou des outils d'analyse (p. ex., Wireshark, tcpdump et SIPp).
- Renforcement de la sécurité de composants et/ou rédaction ou modification de guides portant sur le renforcement de la sécurité de composants.
- Évaluation et mise à l'essai des produits de sécurité des TI par rapport aux exigences de sécurité (p. ex., Critères communs, FIPS 140-2, normes d'assurance élevée).
- Certification CISSP.

PERSPECTIVES DE PLACEMENT

Cyberopérateur Militaires du rang | Temps plein

Les salaires varient de 35,820$ à 77,028$ après 5 ans, selon le niveau

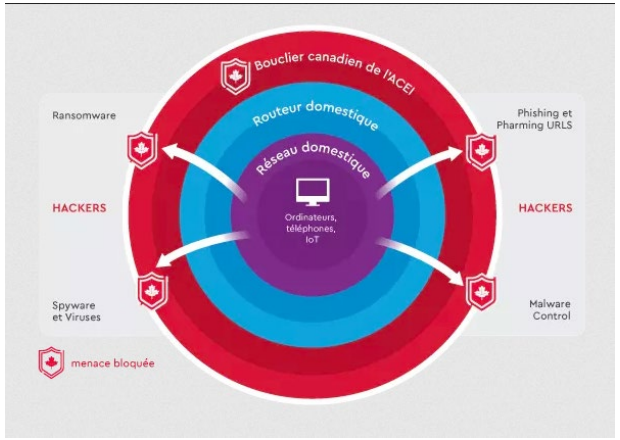
Les cyberopérateurs mènent des cyberopérations défensives et, lorsque cela est nécessaire et faisable, actives.

- Leurs principales responsabilités sont les suivantes :
- Amasser, traiter et analyser des données réseau
- Détecter les vulnérabilités des réseaux
- Gérer un environnement de réseaux informatiques
- Mener des cyberopérations défensives et actives
- Mettre à profit leurs connaissances en matière de sécurité et de communication dans le domaine de la technologie de l'information
- Utiliser et conserver des publications ainsi que des dossiers classifiés et non classifiés

QUAND EST LE BON MOMENT POUR INVESTIR EN SÉCURITÉ INFORMATIQUE?

INITIATIVES DU GC

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ



1. Élaborer un plan d'intervention en cas d'incident
2. Corriger automatiquement tout le contenu
3. Configurer les appareils de manière sécuritaire
4. Activer des logiciels de sécurité
5. Créer des authentifiants robustes
6. Offrir de la formation aux employés
7. Sauvegarder et chiffrer les données
8. Sécuriser les appareils mobiles
9. Établir des défenses périphériques
10. Sécuriser les services de TI impartis
11. Sécuriser les sites Web
12. Mettre en place des contrôles d'accès et des autorisations
13. Sécuriser les dispositifs multimédias portables

Projet de loi C-11 - **Nouveau projet de loi pour protéger la vie privée des Canadiens et accroître leur contrôle sur leurs données et leurs renseignements personnels**

Juridiction	Plus récente mise à jour des lois	Reconnaissance de la vie privée comme droit de la personne	Pouvoir d'établir des règles	Responsabilité démontrable	Pouvoir de rendre des ordonnances	Sanctions administratives pécuniaires	Droit privé d'action
Canada (LPRPDE)	**2015**	✘	✘	✘	✘	✘	✘*
Argentine	2018	✔	✔	✔	✔	✔	✔
Brésil	2018	✔	✔	✔	✔	✔	✔
Union européenne	2018	✔	✔	✔	✔	✔	✔
Royaume-Uni	2018	✔	✔	✔	✔	✔	✔
Australie	2012	✔	✔	✔	✔	✔	✔
Mexique	2016	✔	✔	✔	✔	✔	✘
Corée du Sud	2018	✔	✔	✔	✔	✔	✘
Nouvelle-Zélande	2020	✔	✔	✔	✔	✘	✘
Singapour	2012	✘	✔	✔	✔	✔	✔
Japon	2015	✘	✔	✔	✔	✔	✘
Californie (California Consumer Protection Act)	2019	✘	✔	✔	✘	✔	✔

✔ = oui ✘ = non

* La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) prévoit actuellement le droit pour les personnes d'amener une organisation devant la Cour fédérale pour obtenir des réparations, telles qu'une ordonnance obligeant l'organisation à corriger ses pratiques et/ou à accorder des dommages-intérêts, mais seulement après une enquête et un rapport de conclusions du Commissariat à la protection de la vie privée du Canada, ou un avis de fin d'examen.

Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

INITIATIVES DU GQ

ASSEMBLÉE NATIONALE
DU QUÉBEC

PREMIÈRE SESSION — QUARANTE-DEUXIÈME LÉGISLATURE

Projet de loi n° 64

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

ASSEMBLÉE NATIONALE
DU QUÉBEC

PREMIÈRE SESSION — QUARANTE-DEUXIÈME LÉGISLATURE

Projet de loi n° 53

Loi sur les agents d'évaluation du crédit

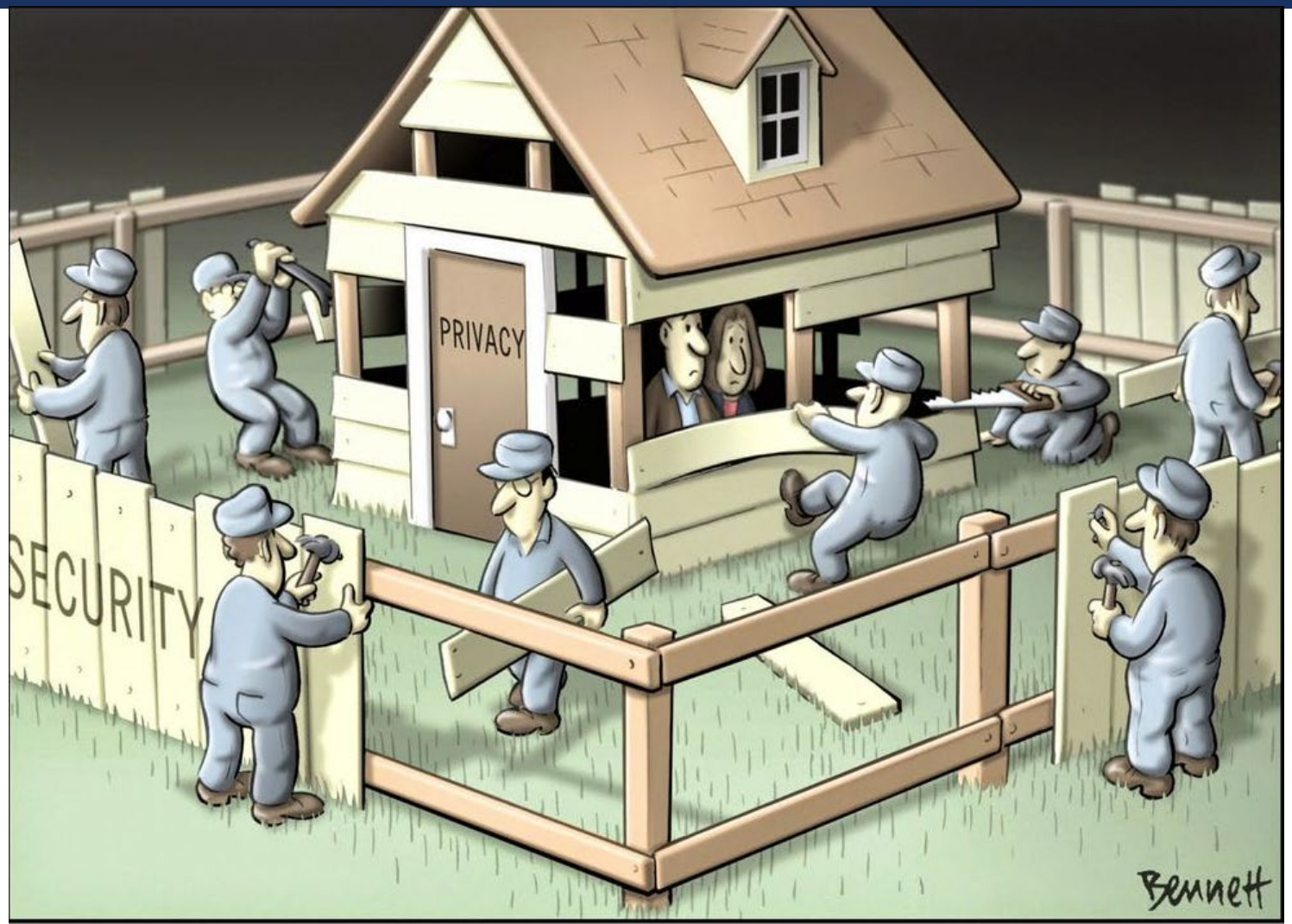
Votre gouvernement

Québec

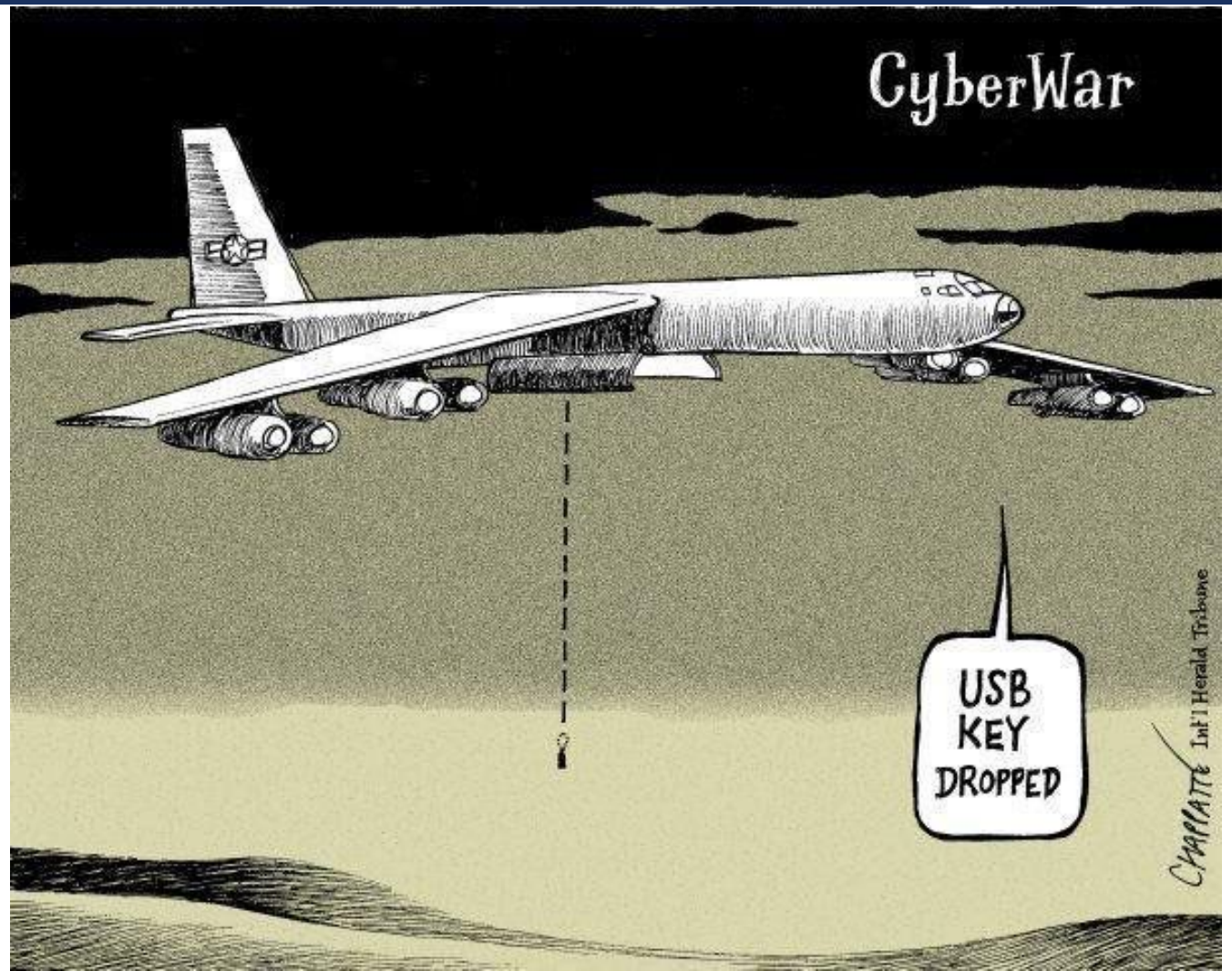
ATN Académie de la transformation numérique

CONCLUSION

UN CHOIX À FAIRE ?



RÉALITÉ DES CONFLITS D'AUJOURD'HUI ET DE DEMAIN



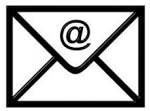

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
KEININGERS ©2000 THE CHARLOTTE OBSERVER
Geeks
HACK
HACK
HACK
HACK

Capt(ret) Steve Waterhouse, CD

INFOSECSW, inc

https://www.infosecsw.ca

Steve Waterhouse, CD, CISSP
Montréal, Canada



info@infosecsw.ca
PGP:0x0696B43D

@Water_Steve

@cyberstevewater

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

A PRAGMATIC VIEW OF IMPLEMENTING ZERO TRUST

BOB KALKA
Vice President
IBM Security

IBM

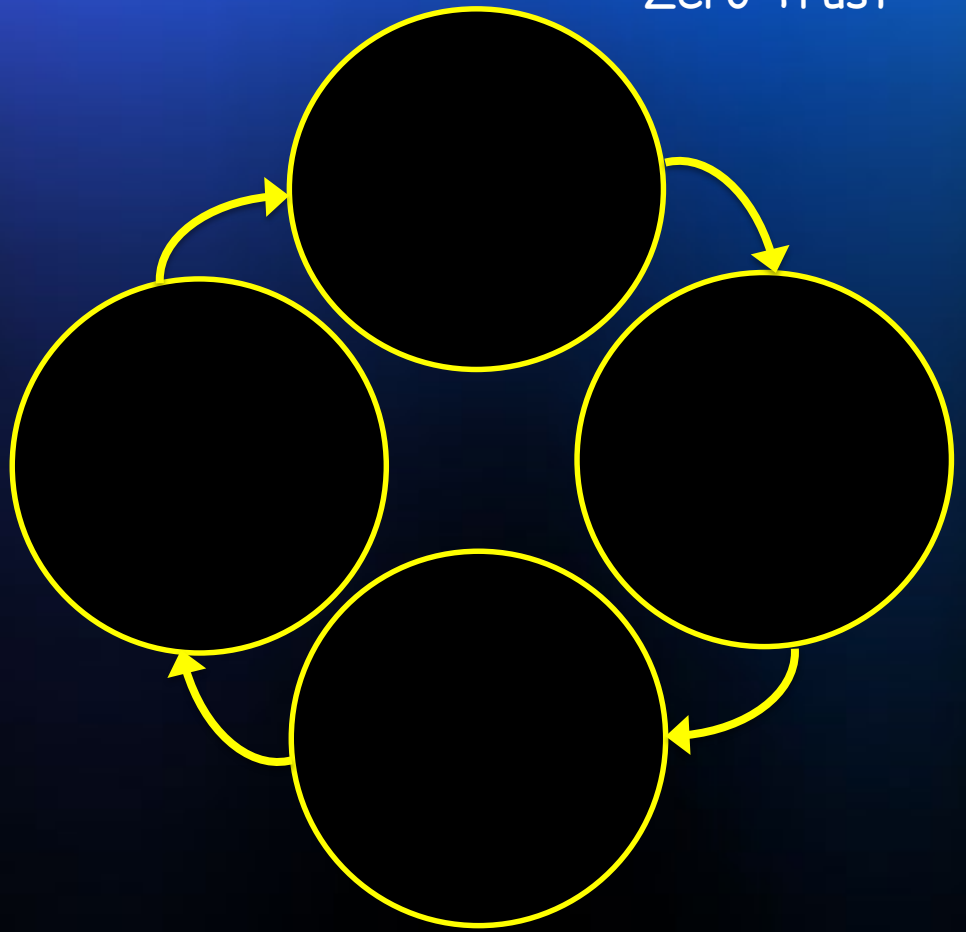
CYBER SECURITY CONFERENCE

2020

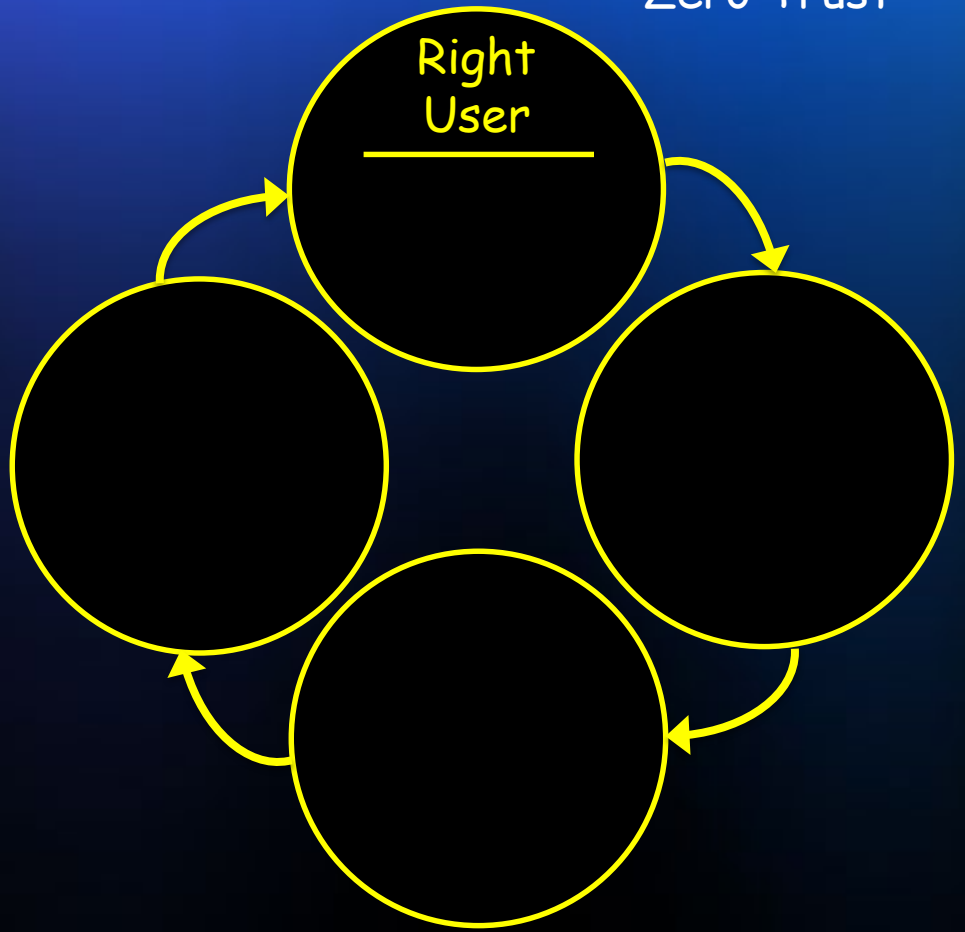
VIRTUAL EDITION

Zero Trust

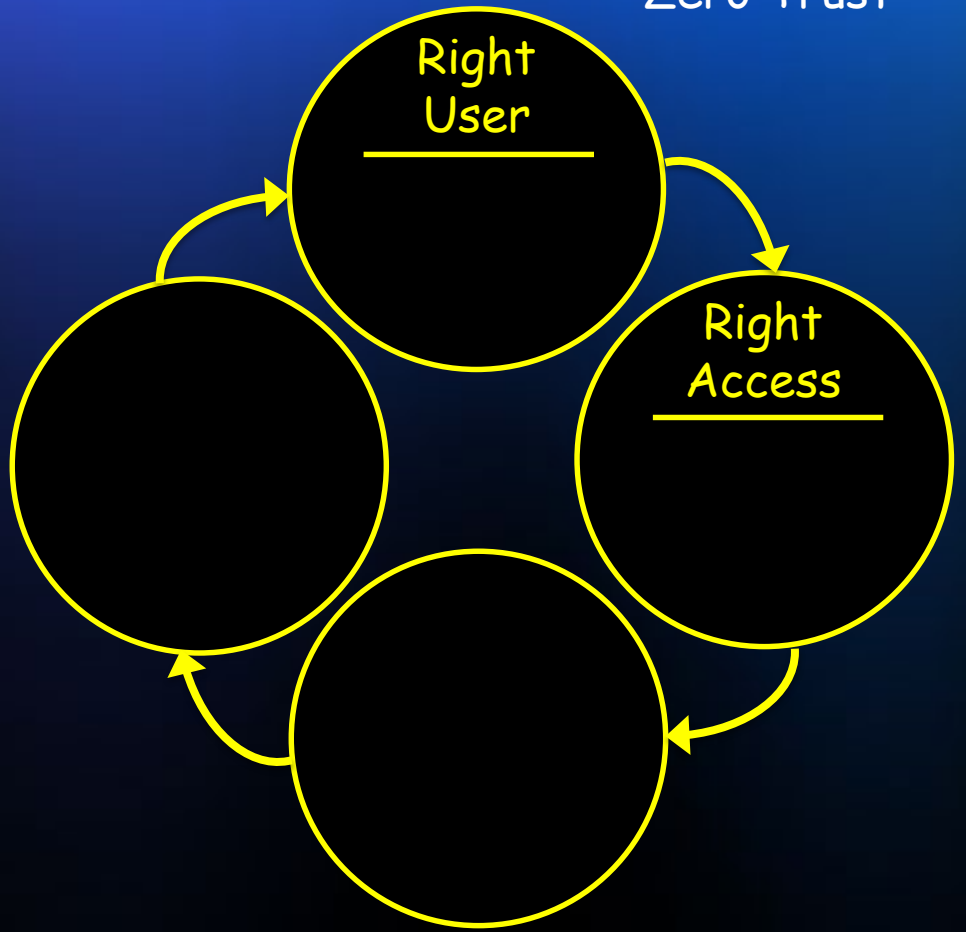
Zero Trust



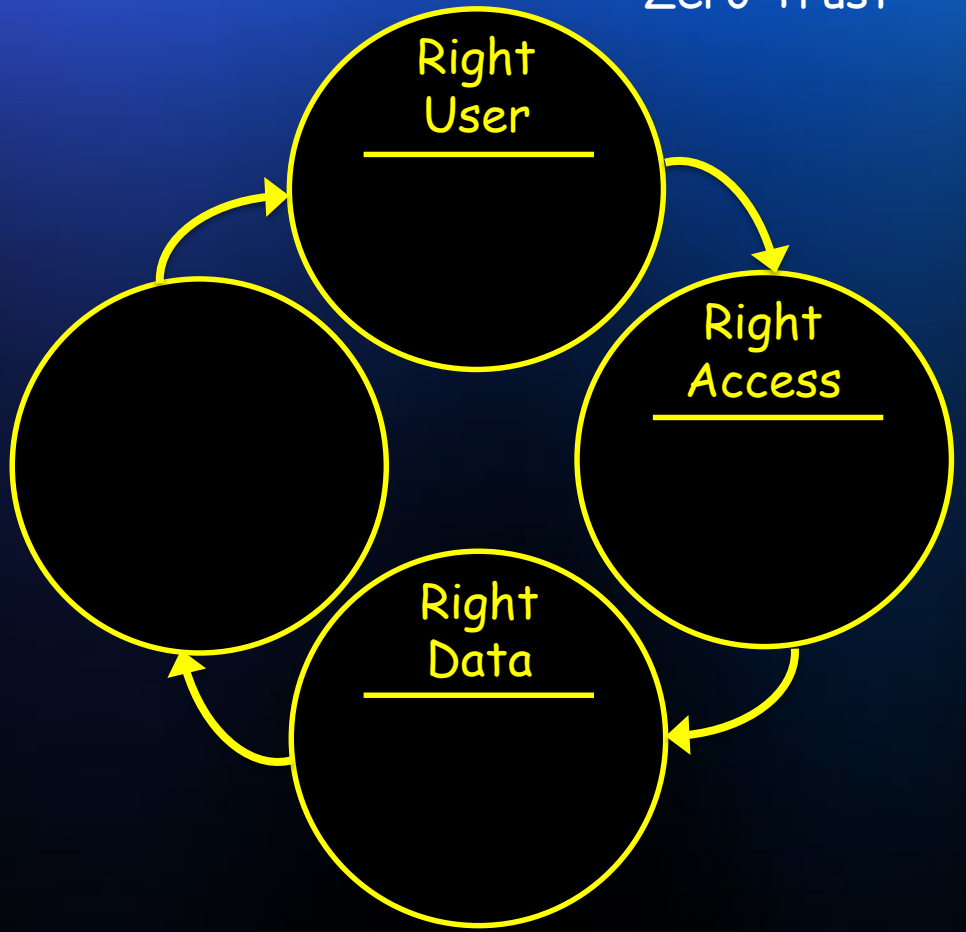
Zero Trust



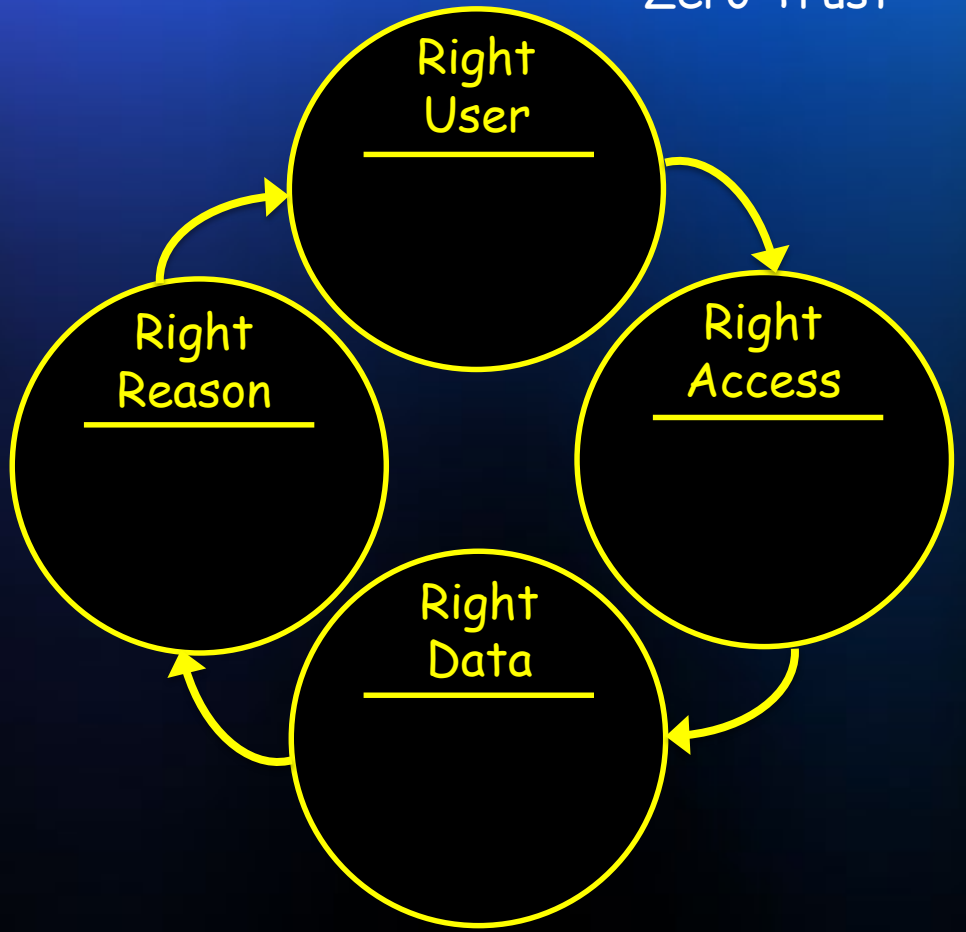
Zero Trust



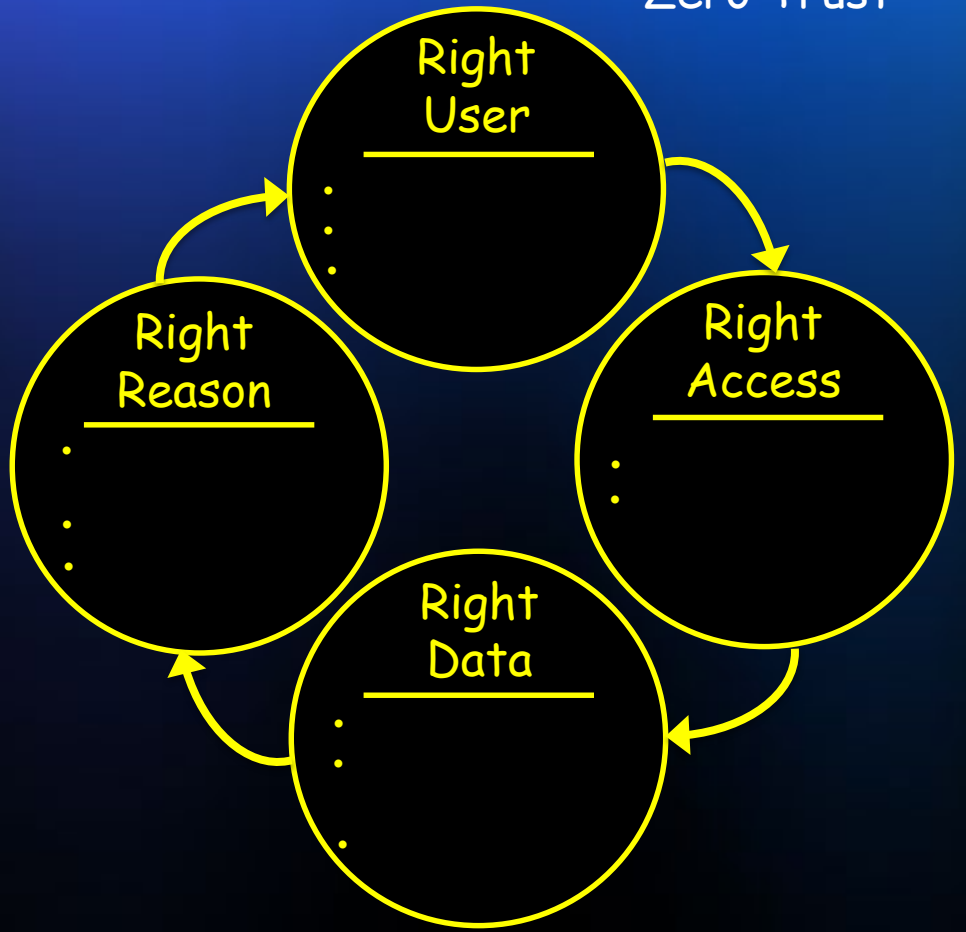
Zero Trust



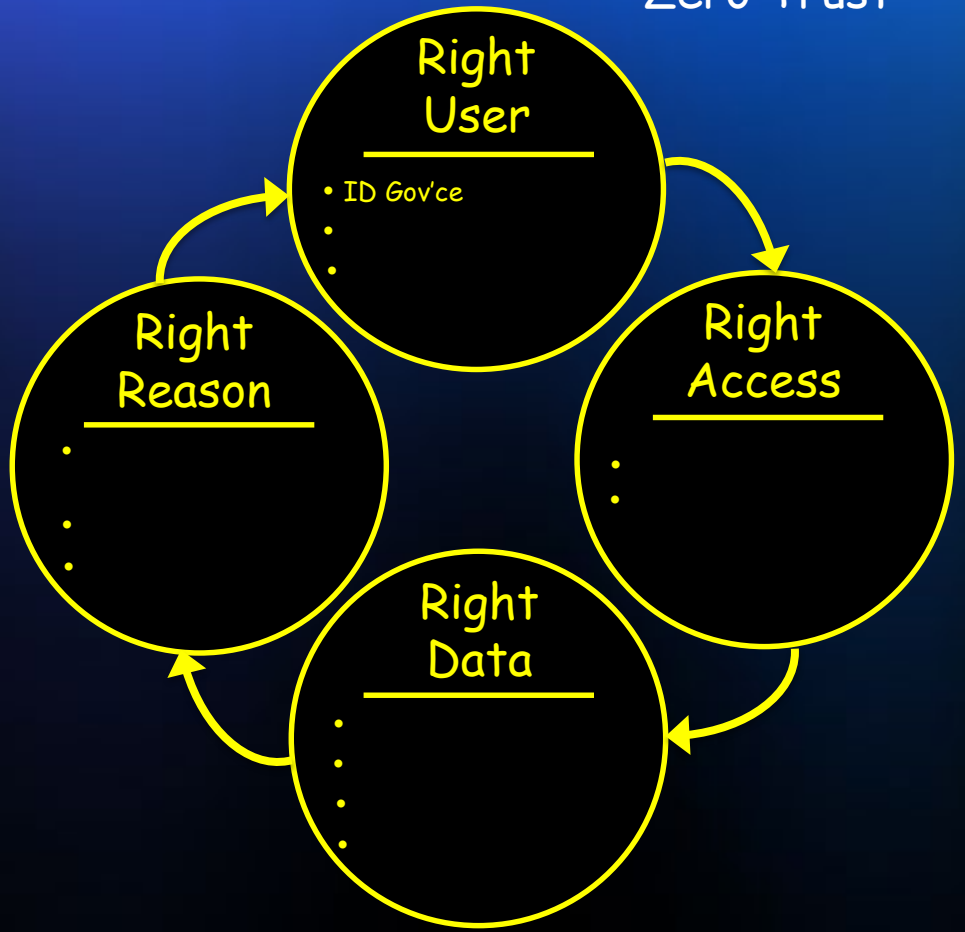
Zero Trust



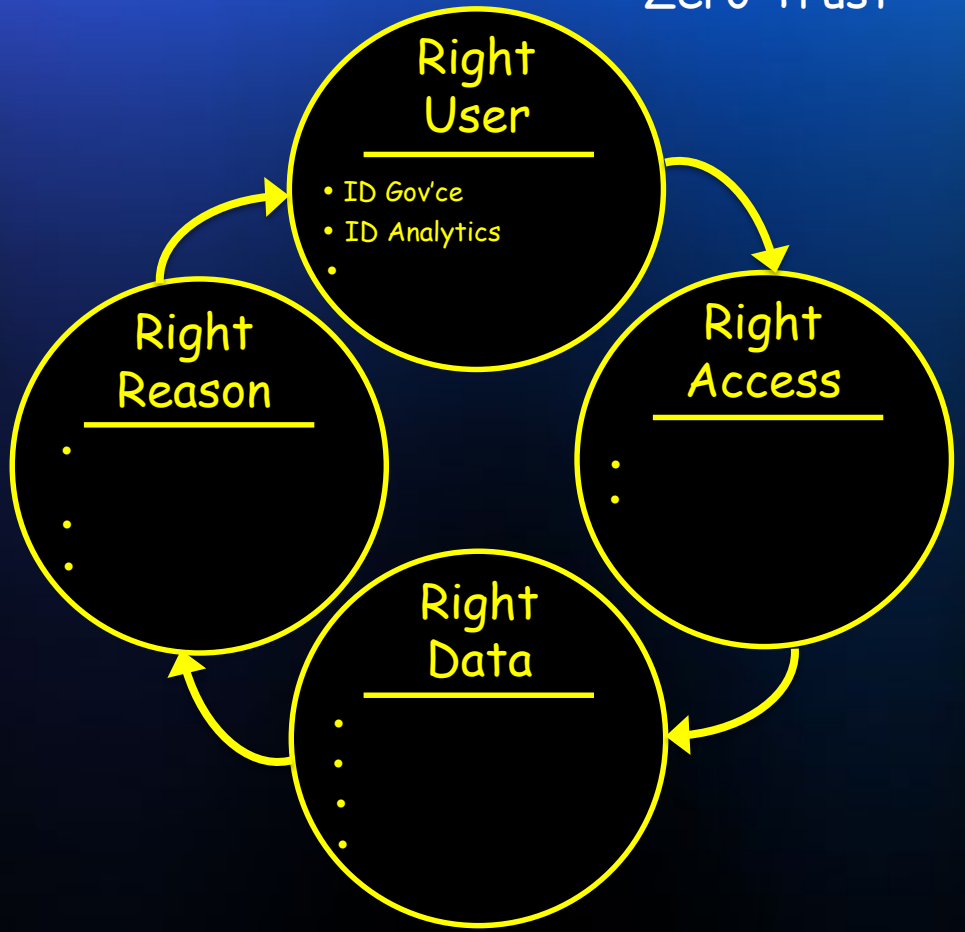
Zero Trust



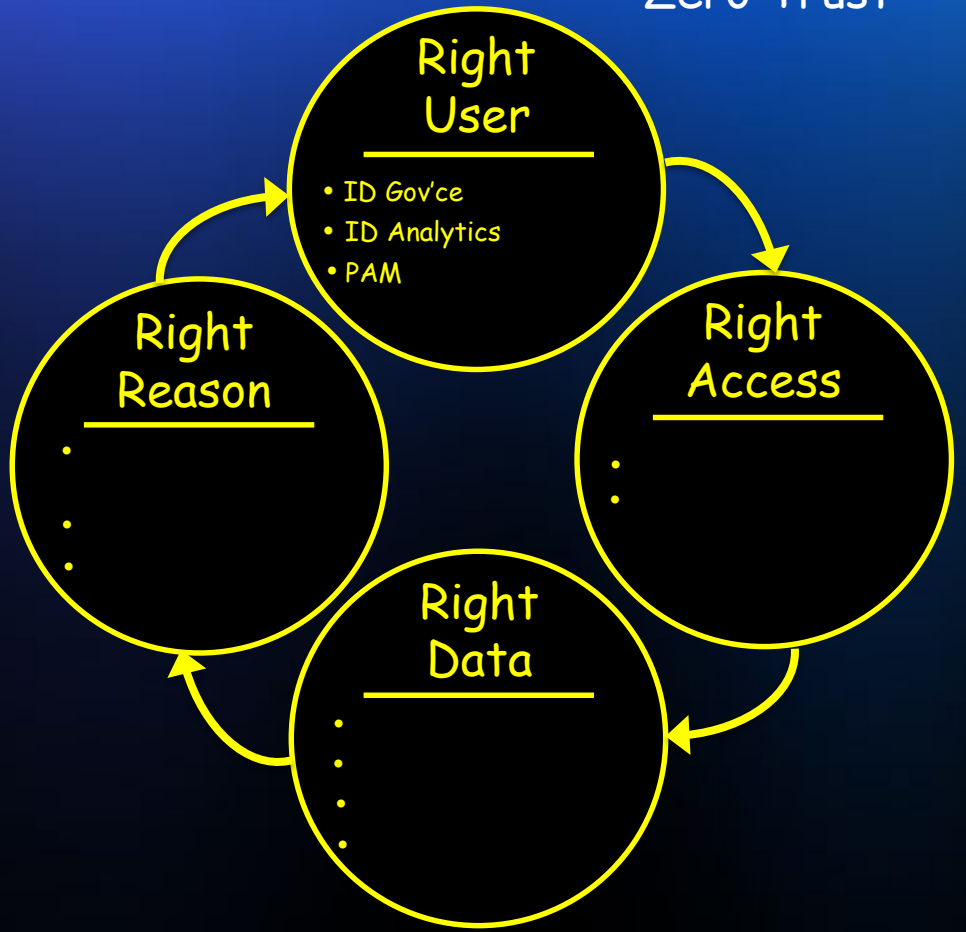
Zero Trust



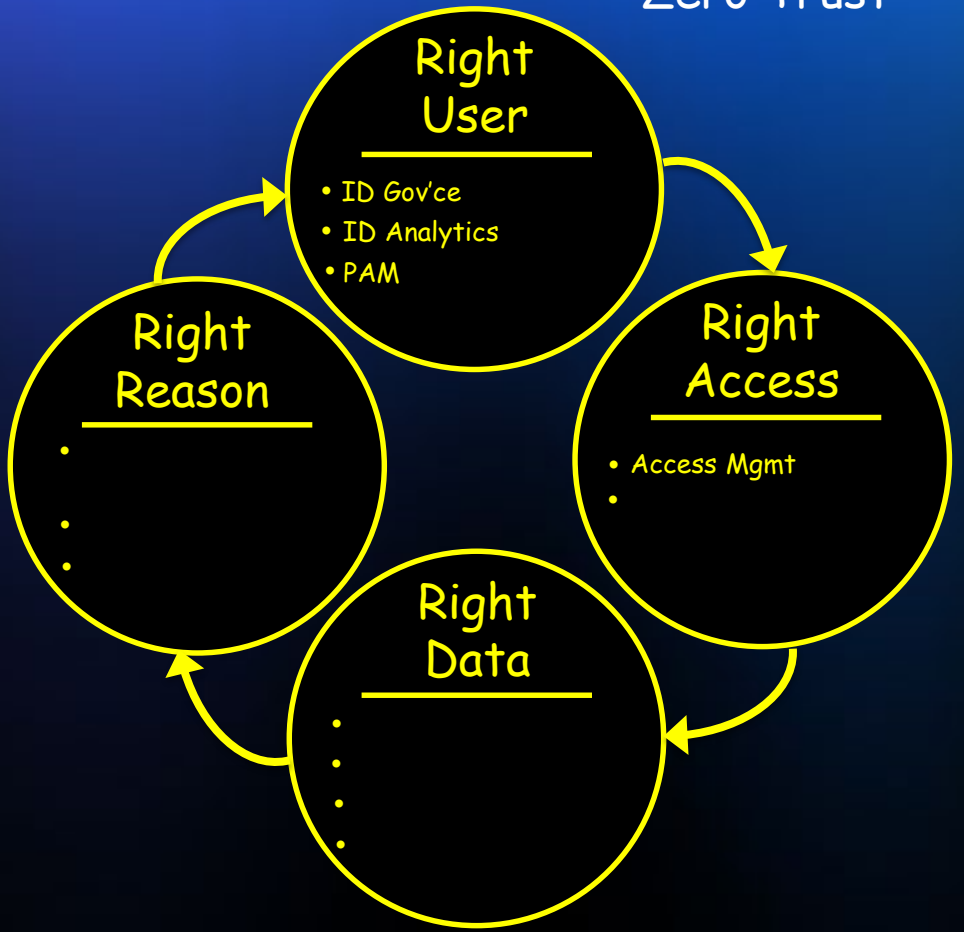
Zero Trust


Right
User
• ID Gov'ce
• ID Analytics
Right
Access
Right
Data
Right
Reason

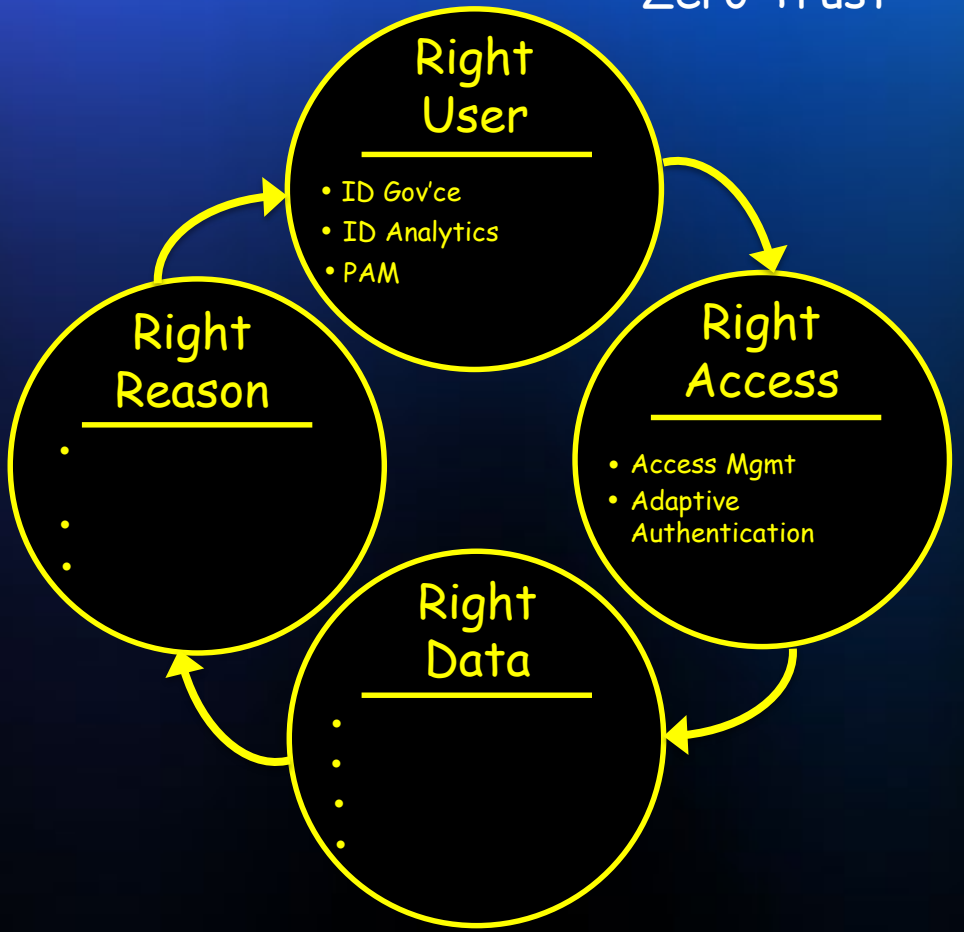
Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
Right Data
Right Reason

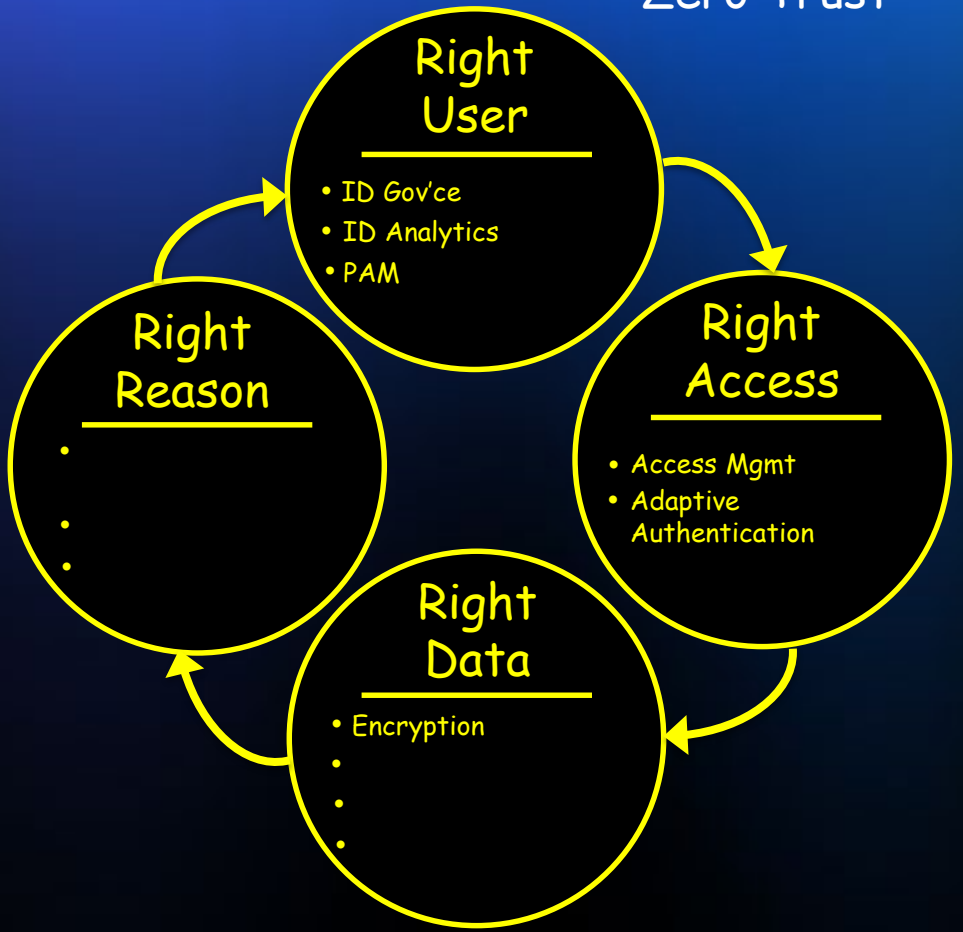
Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
Right Data
Right Reason

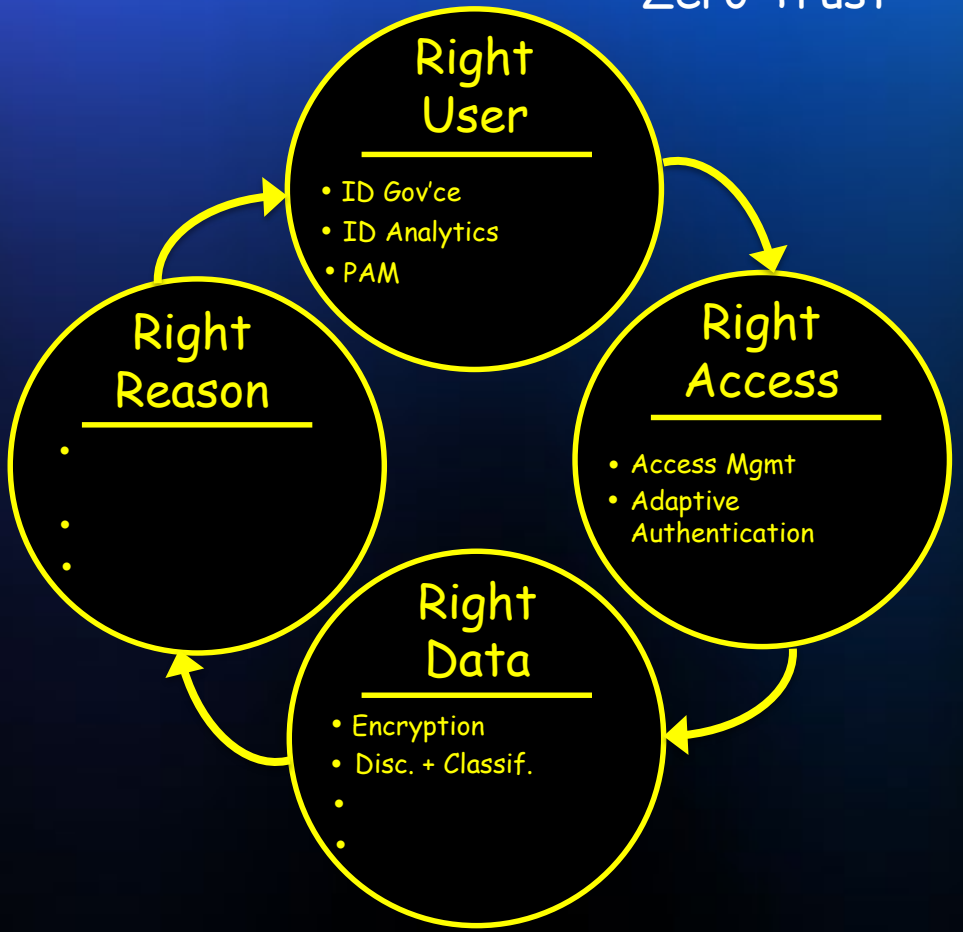
Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
Right Reason

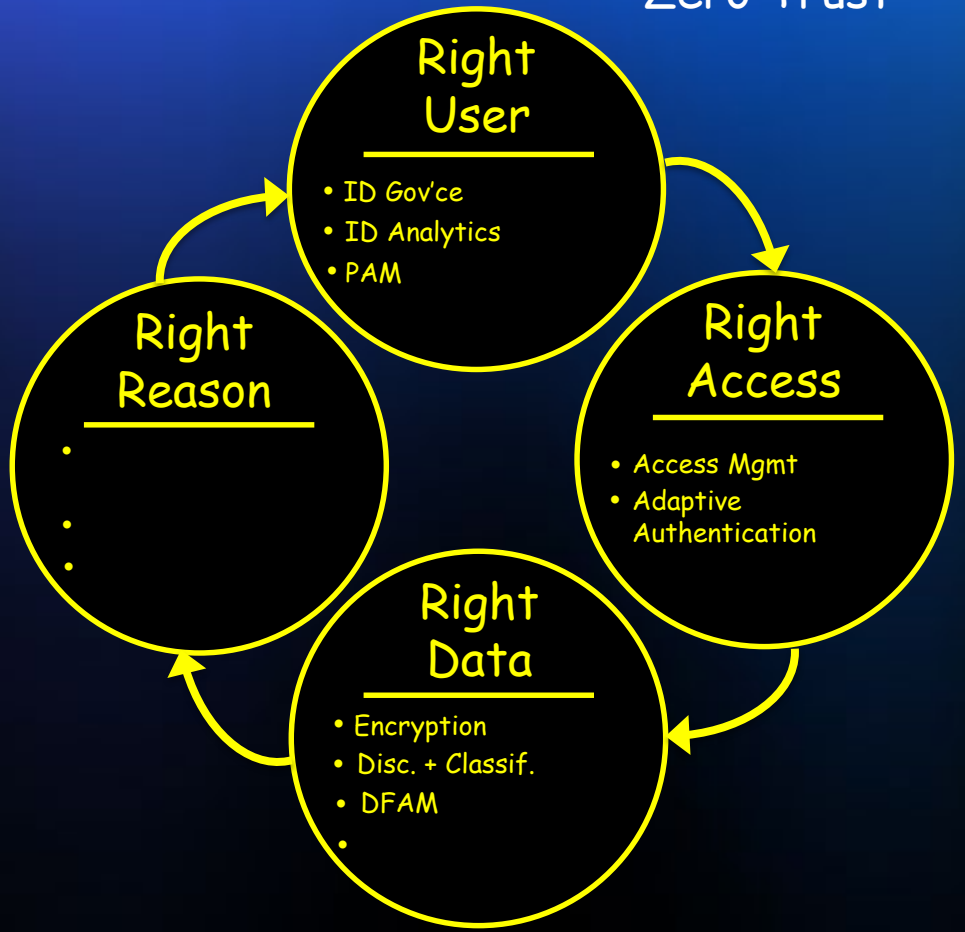
Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
Right Reason

Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
• Disc. + Classif.
Right Reason

Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
• Disc. + Classif.
• DFAM
•
Right Reason
•
•
•

Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
• Disc. + Classif.
• DFAM
• Key Mgmt
Right Reason
•
•
•

Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
• Disc. + Classif.
• DFAM
• Key Mgmt
Right Reason
• Data Risk Insights
•
•

Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
• Disc. + Classif.
• DFAM
• Key Mgmt
Right Reason
• Data Risk Insights
• Fraud
•

Zero Trust


Right User
• ID Gov'ce
• ID Analytics
• PAM
Right Access
• Access Mgmt
• Adaptive Authentication
Right Data
• Encryption
• Disc. + Classif.
• DFAM
• Key Mgmt
Right Reason
• Data Risk Insights
• Fraud
• Config/ Mgmt

MODERNIZE

Zero Trust

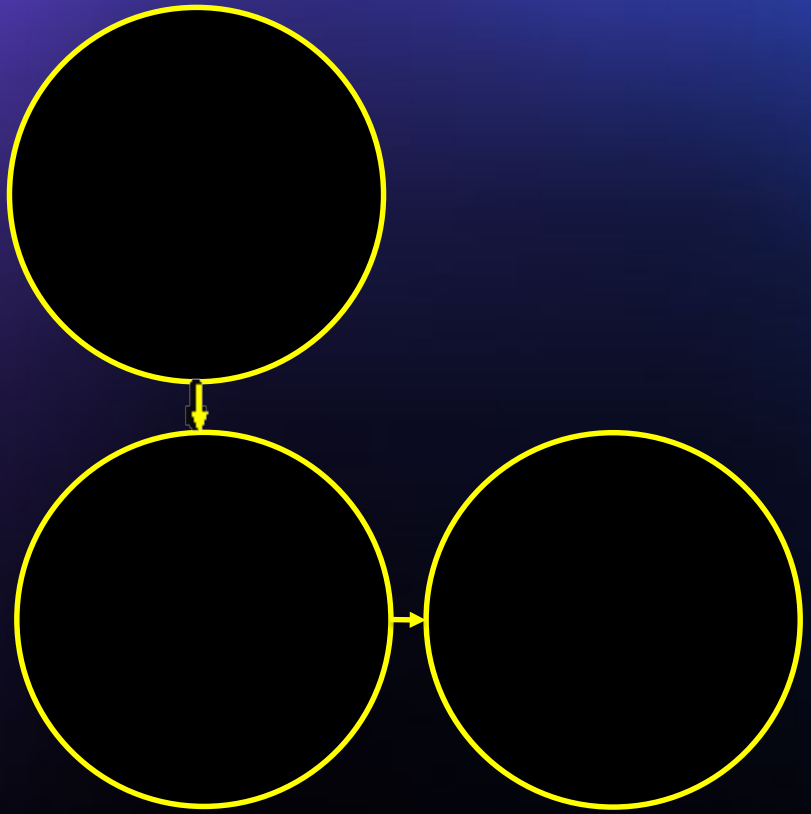
MODERNIZE

Threat Management

Zero Trust

MODERNIZE

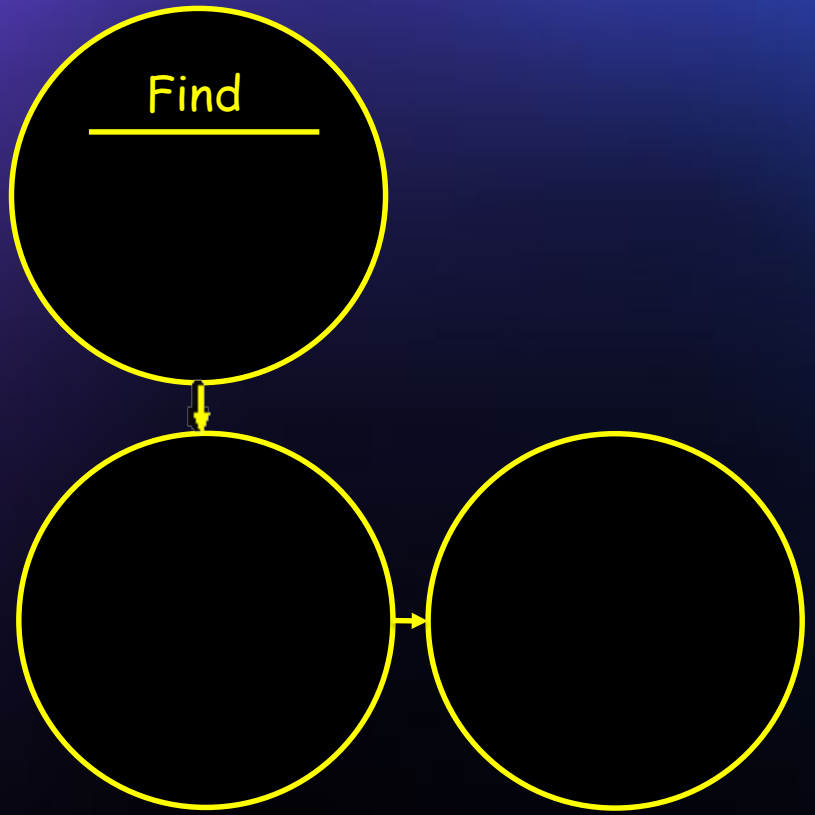
Threat Management



Zero Trust

MODERNIZE

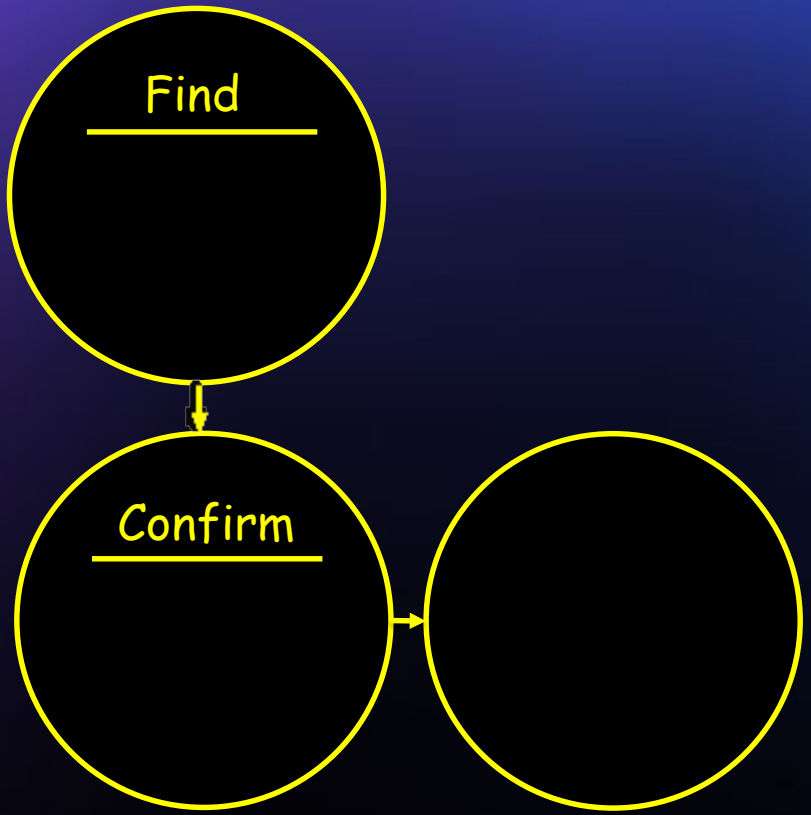
Threat Management



Zero Trust

MODERNIZE

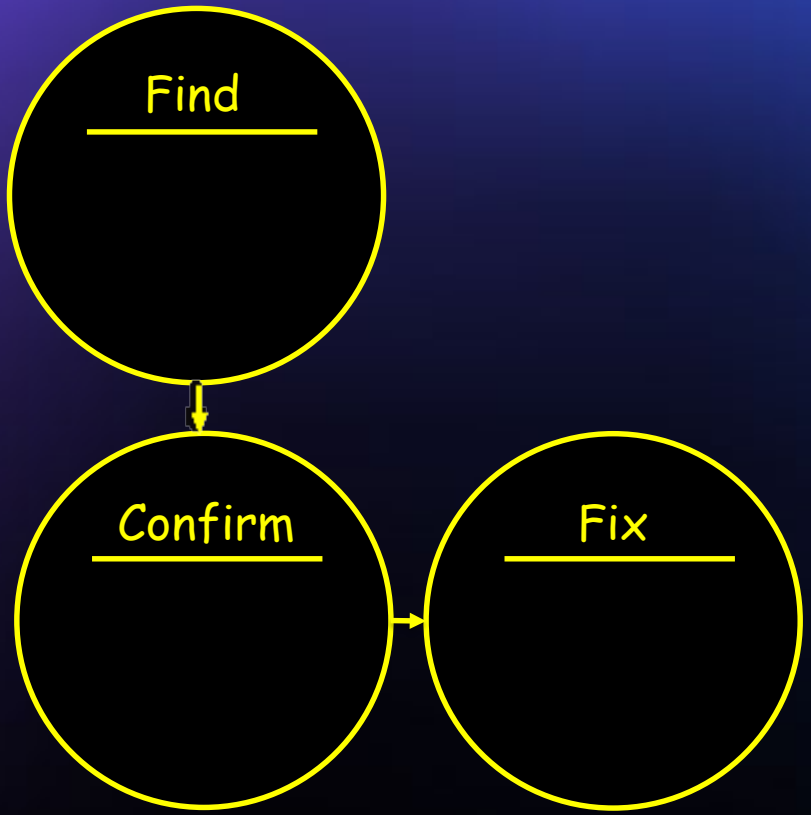
Threat Management



Zero Trust

MODERNIZE

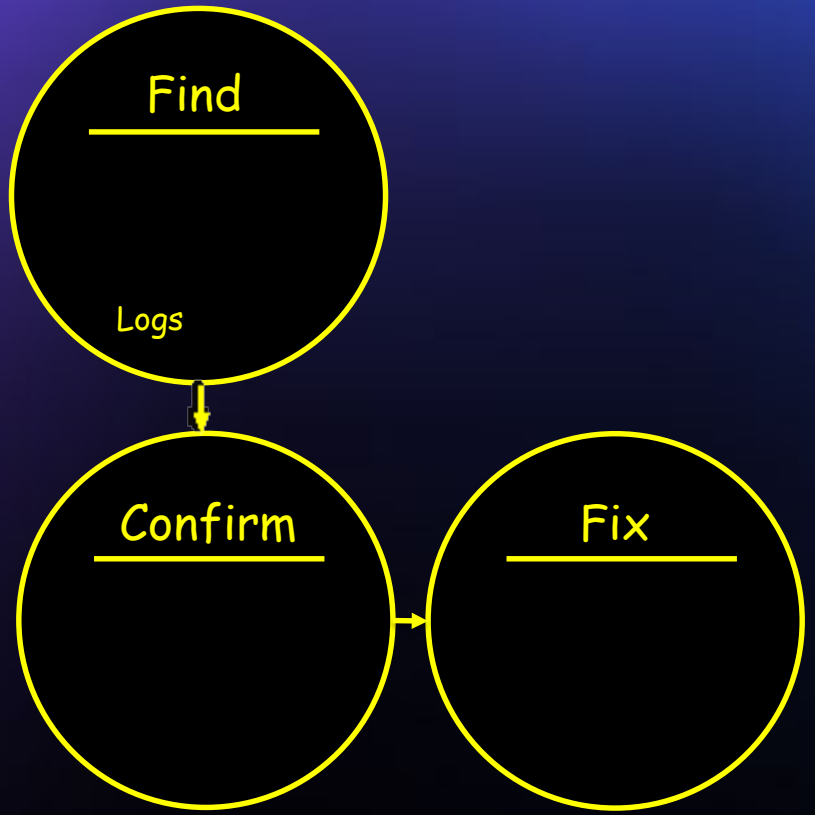
Threat Management



Zero Trust

MODERNIZE

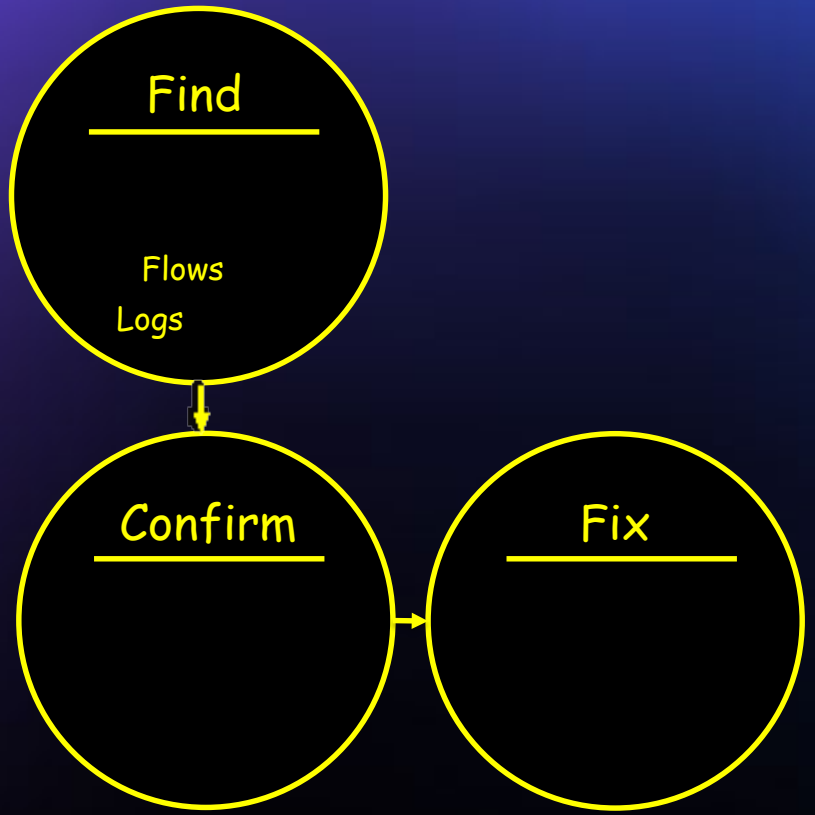
Threat Management



Zero Trust

MODERNIZE

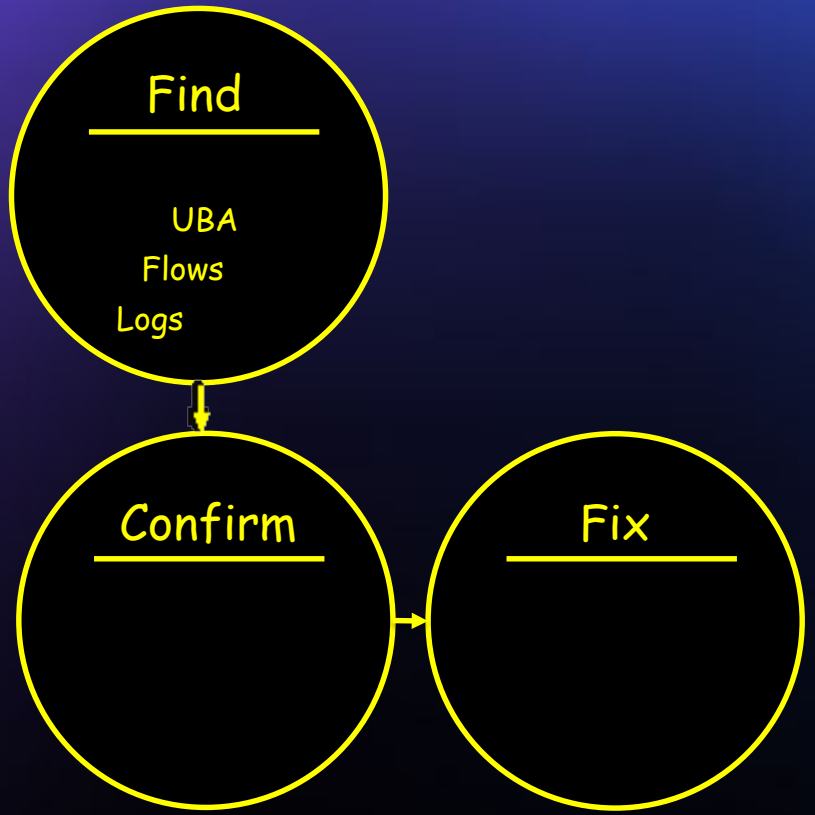
Threat Management



Zero Trust

MODERNIZE

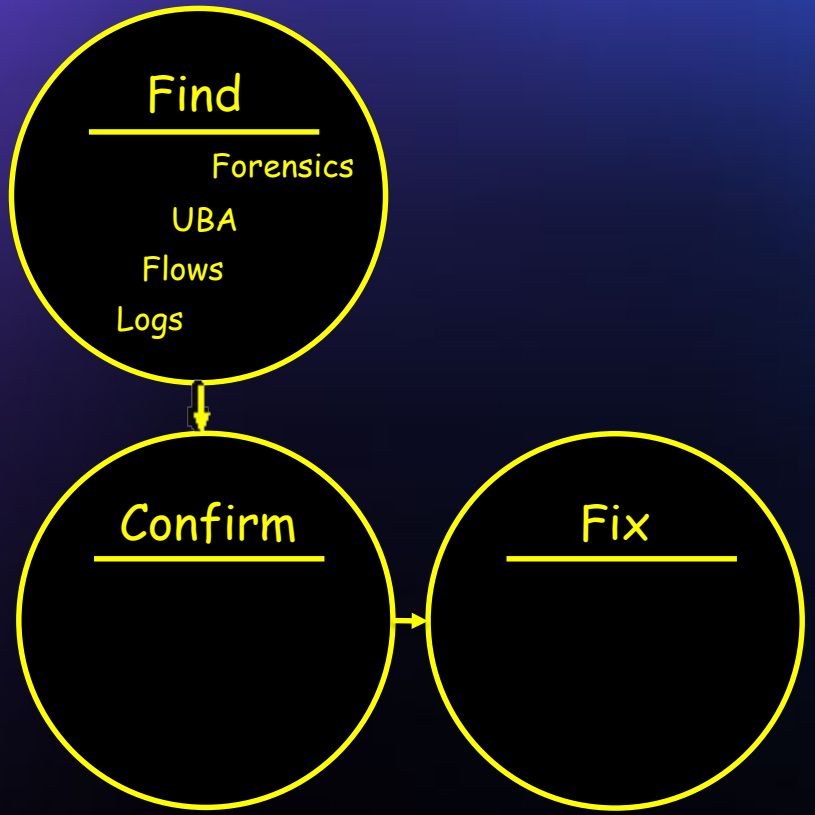
Threat Management



Zero Trust

MODERNIZE

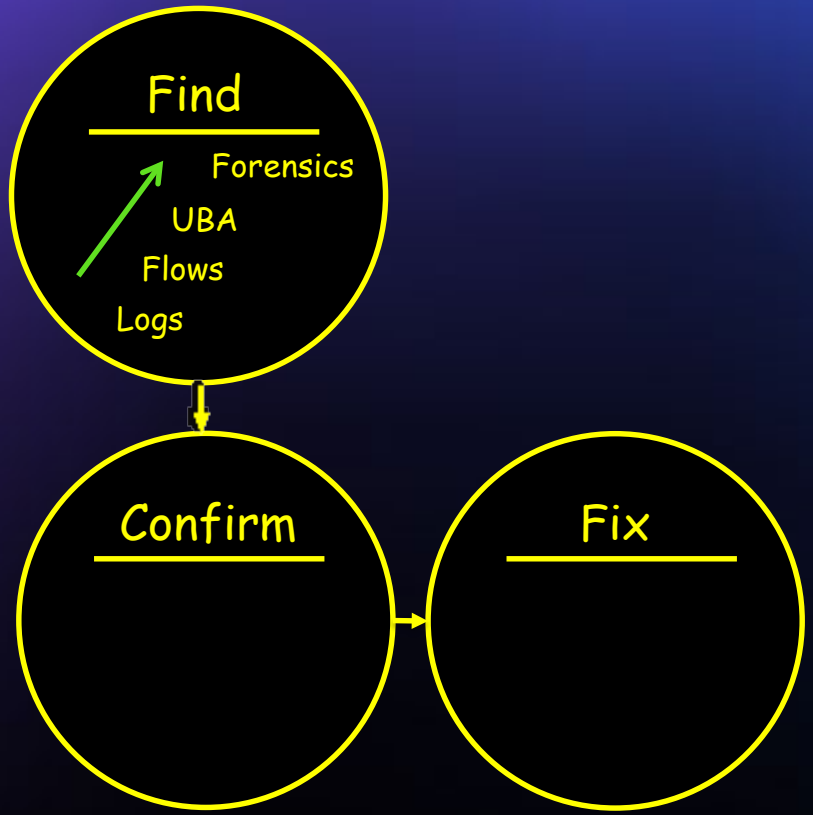
Threat Management



Zero Trust

MODERNIZE

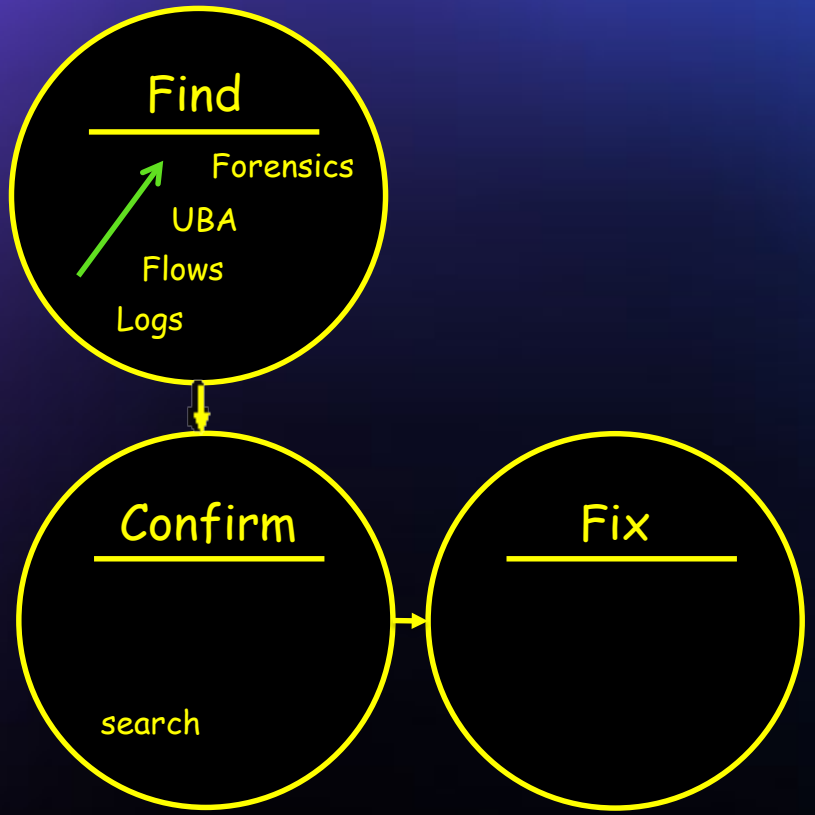
Threat Management



Zero Trust

MODERNIZE

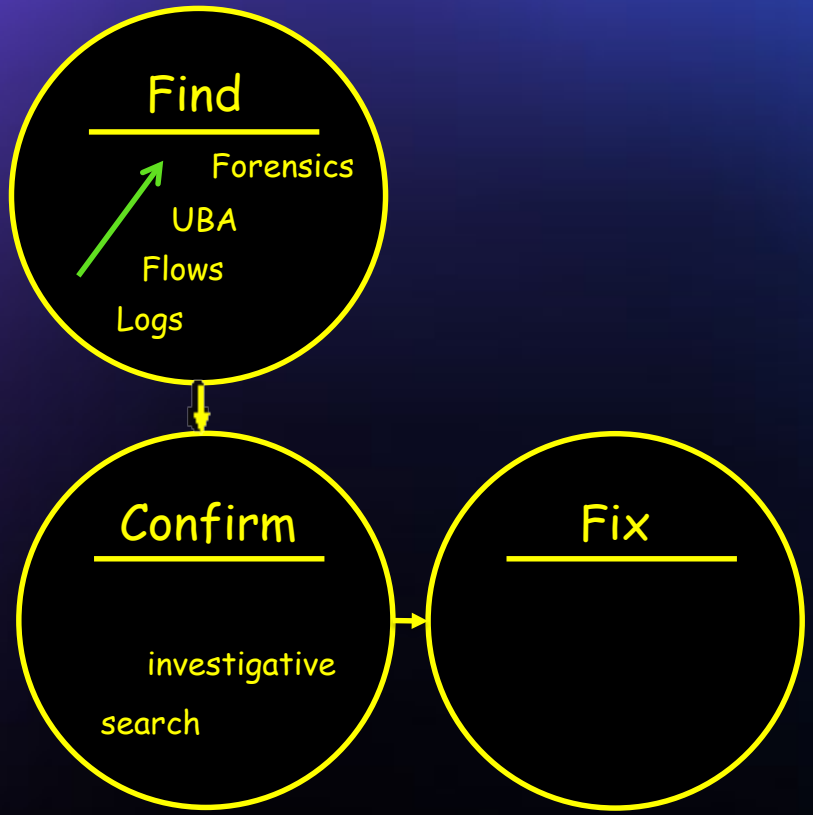
Threat Management



Zero Trust

MODERNIZE

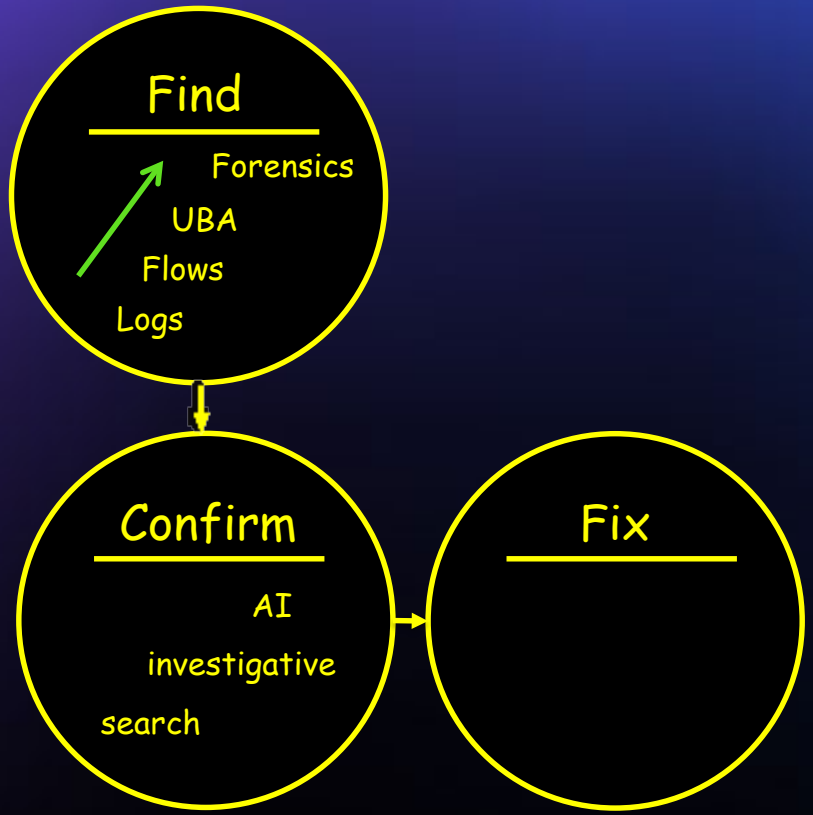
Threat Management



Zero Trust

MODERNIZE

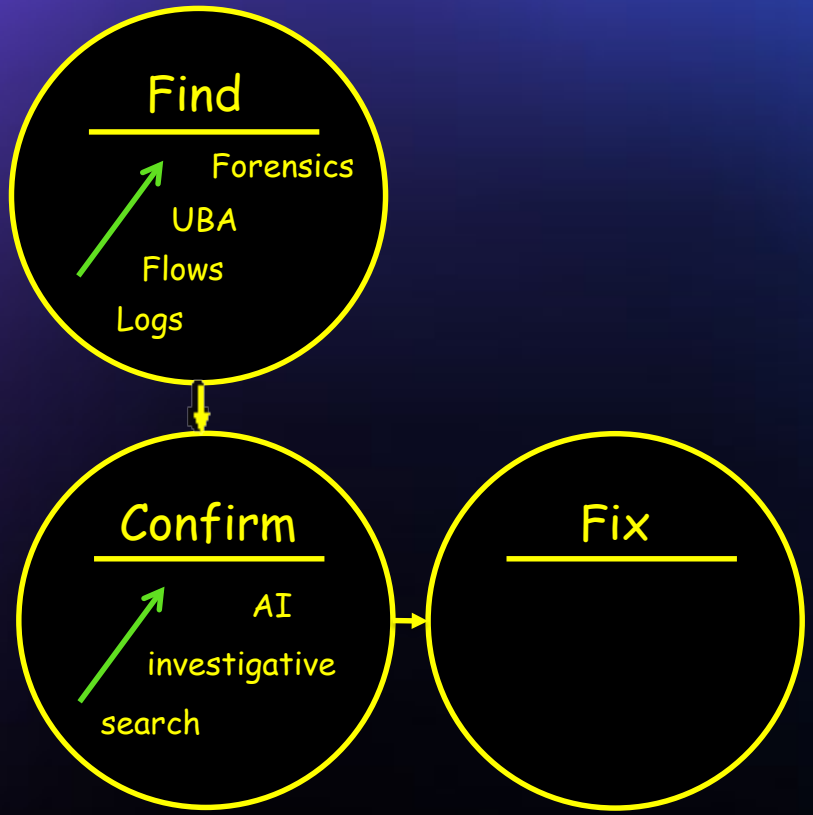
Threat Management



Zero Trust

MODERNIZE

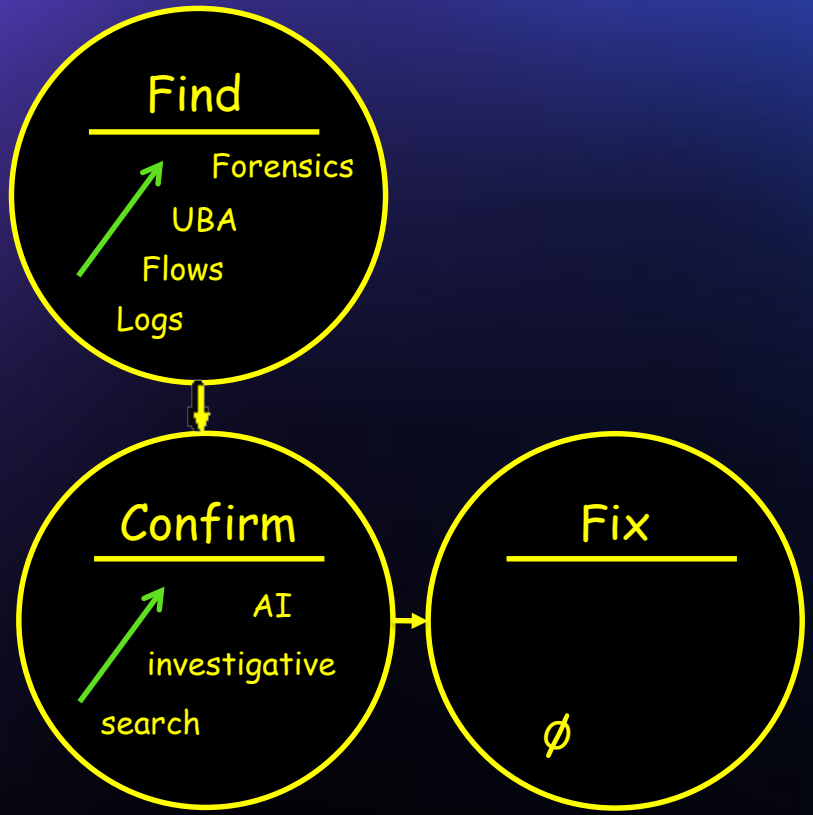
Threat Management



Zero Trust

MODERNIZE

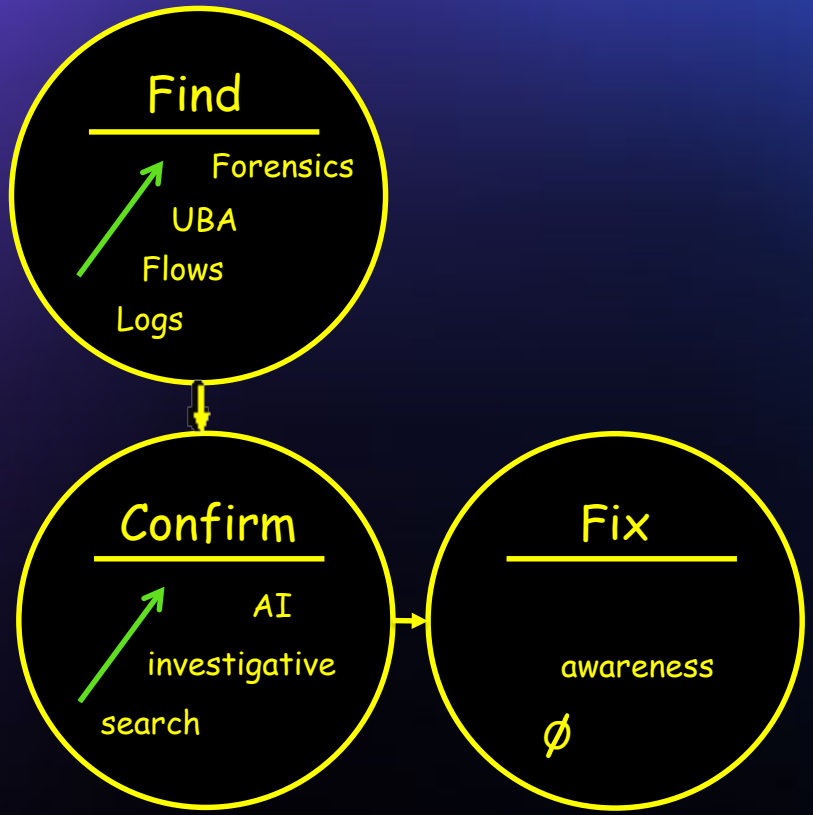
Threat Management



Zero Trust

MODERNIZE

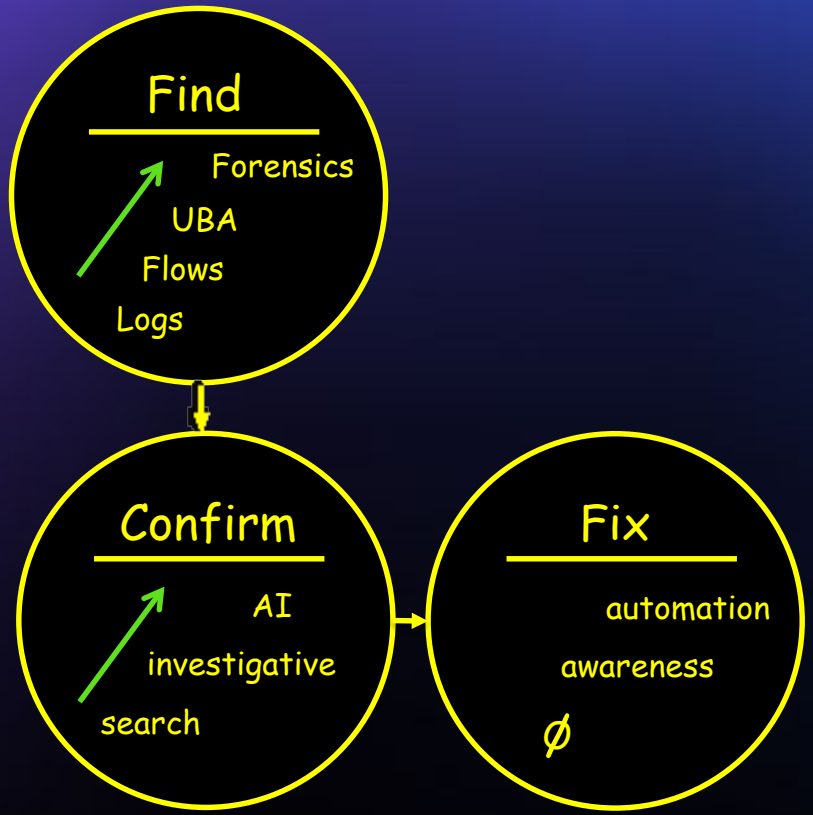
Threat Management



Zero Trust

MODERNIZE

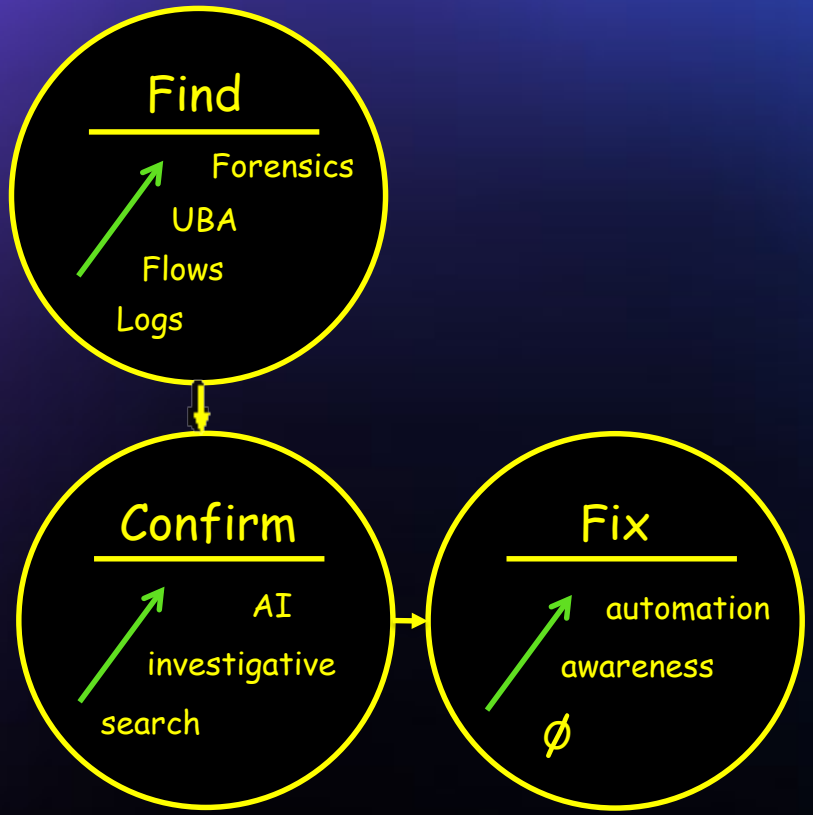
Threat Management



Zero Trust

MODERNIZE

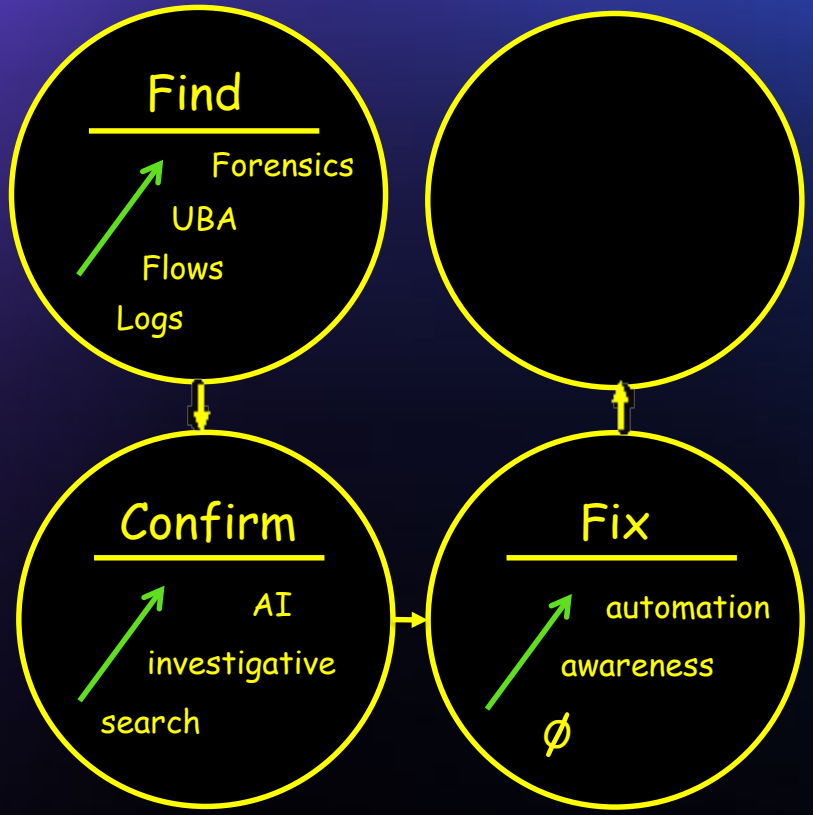
Threat Management



Zero Trust

MODERNIZE

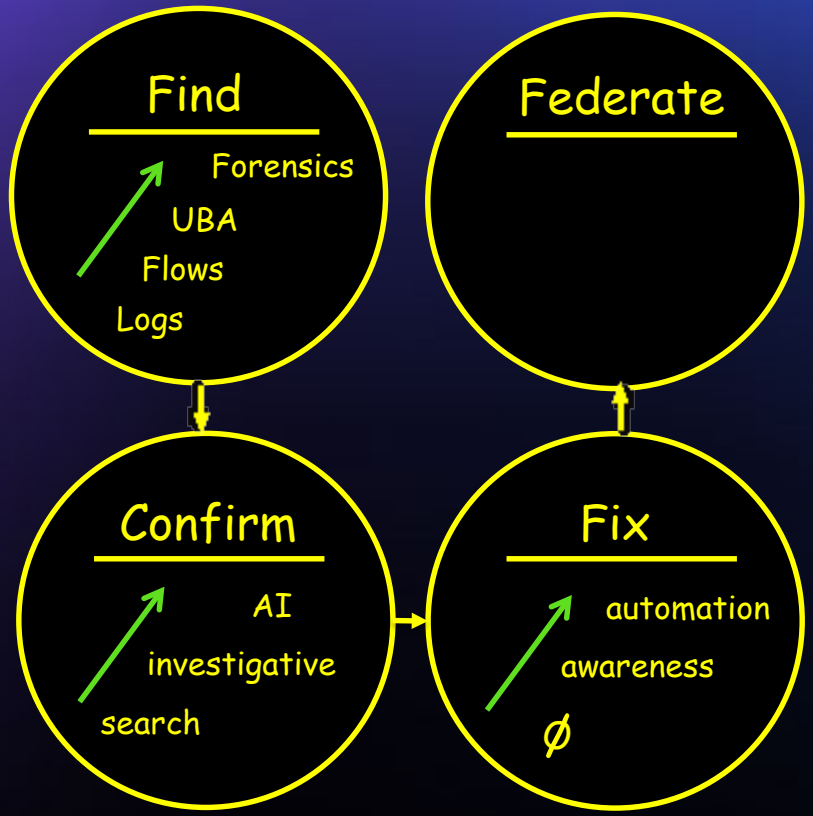
Threat Management



Zero Trust

MODERNIZE

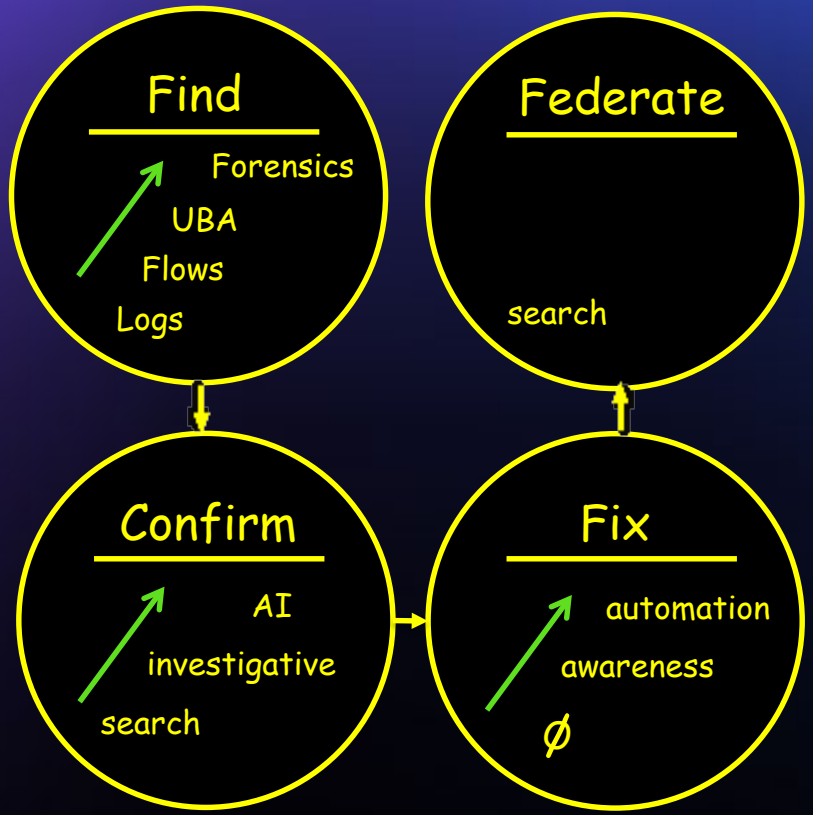
Threat Management



Zero Trust

MODERNIZE

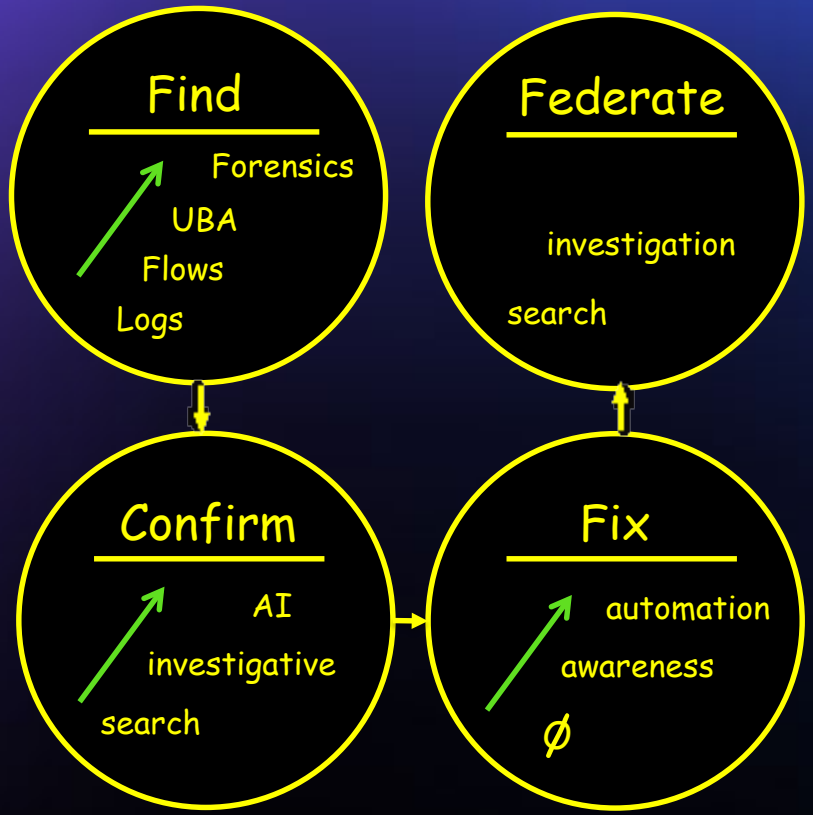
Threat Management



Zero Trust

MODERNIZE

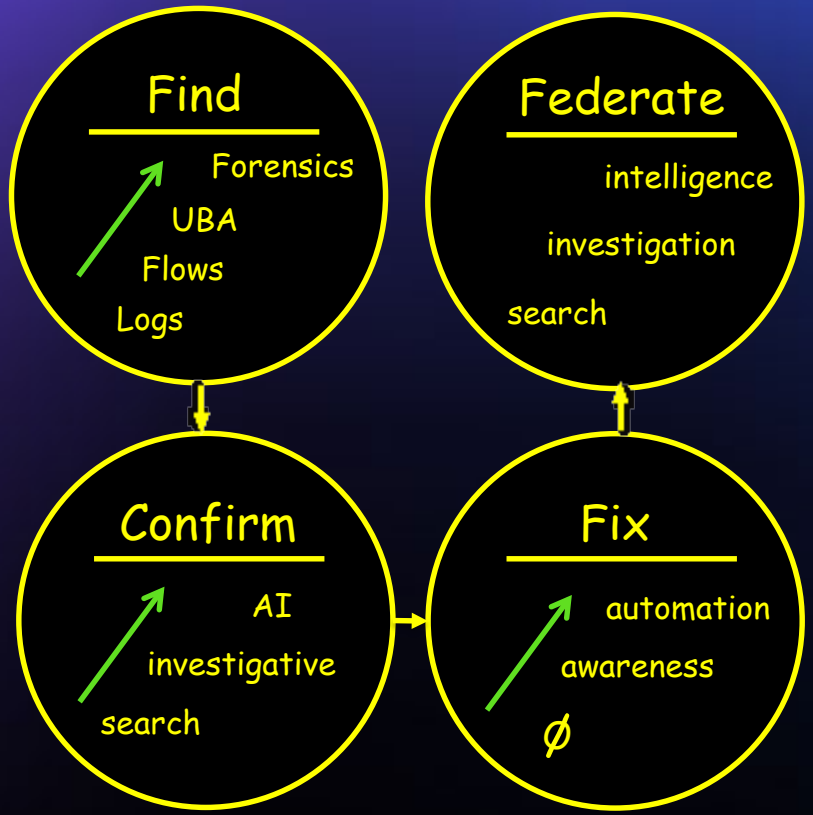
Threat Management



Zero Trust

MODERNIZE

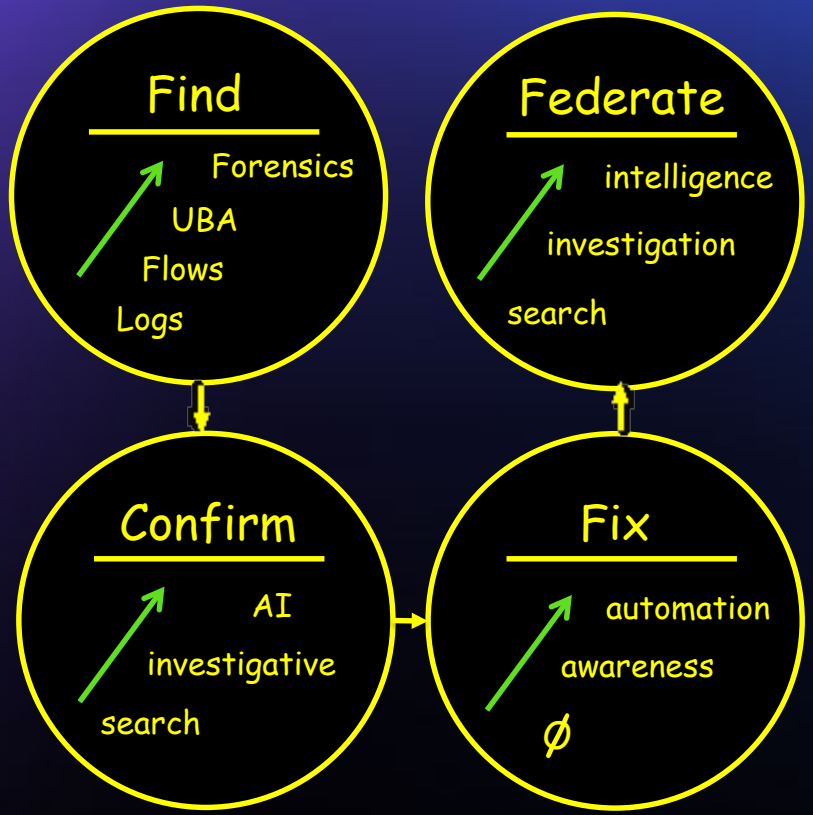
Threat Management



Zero Trust

MODERNIZE

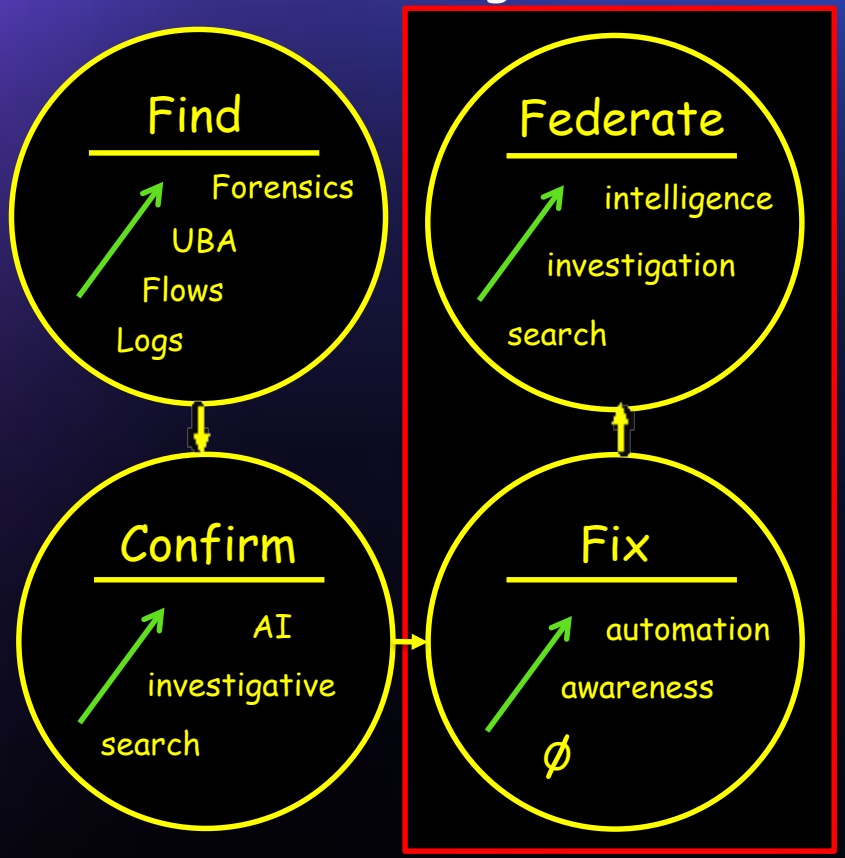
Threat Management



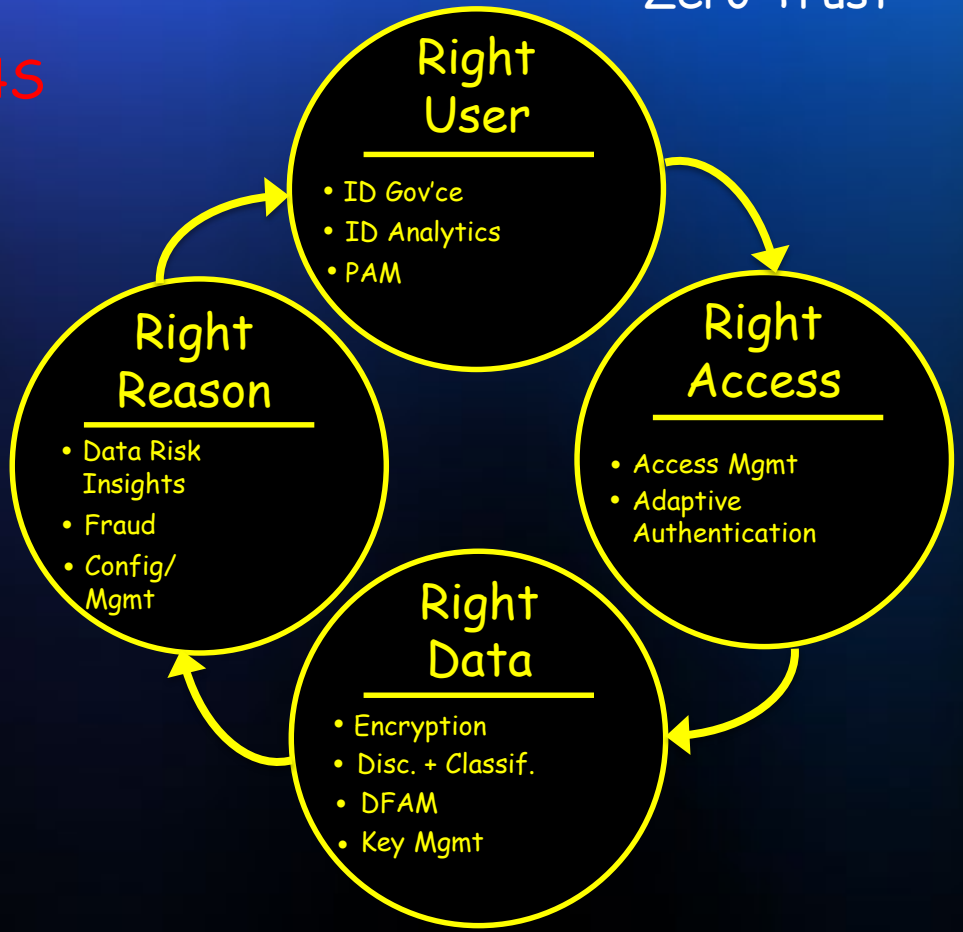
Zero Trust

MODERNIZE

Threat Management



Zero Trust



MODERNIZE

Threat Management

CP4S

Find
- Forensics
- UBA
- Flows
- Logs

Federate
- intelligence
- investigation
- search

Confirm
- AI
- investigative
- search

Fix
- automation
- awareness
- Ø

A

Zero Trust

Right User
- ID Gov'ce
- ID Analytics
- PAM

Right Access
- Access Mgmt
- Adaptive Authentication

Right Data
- Encryption
- Disc. + Classif.
- DFAM
- Key Mgmt

Right Reason
- Data Risk Insights
- Fraud
- Config/ Mgmt

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

CYBERSECURITY IN THE NEW NORMAL

CYBER SECURITY CONFERENCE 2020 VIRTUAL EDITION

KEVIN PEUHKURINEN
Principal Research Director – Security, Risk & Compliance

INFO-TECH RESEARCH GROUP

ASIA PACIFIC / SCIENCE & HEALTH

Outbreak of SARS-like pneumonia being investigated in China

AFP-JIJI

 Dec 31, 2019

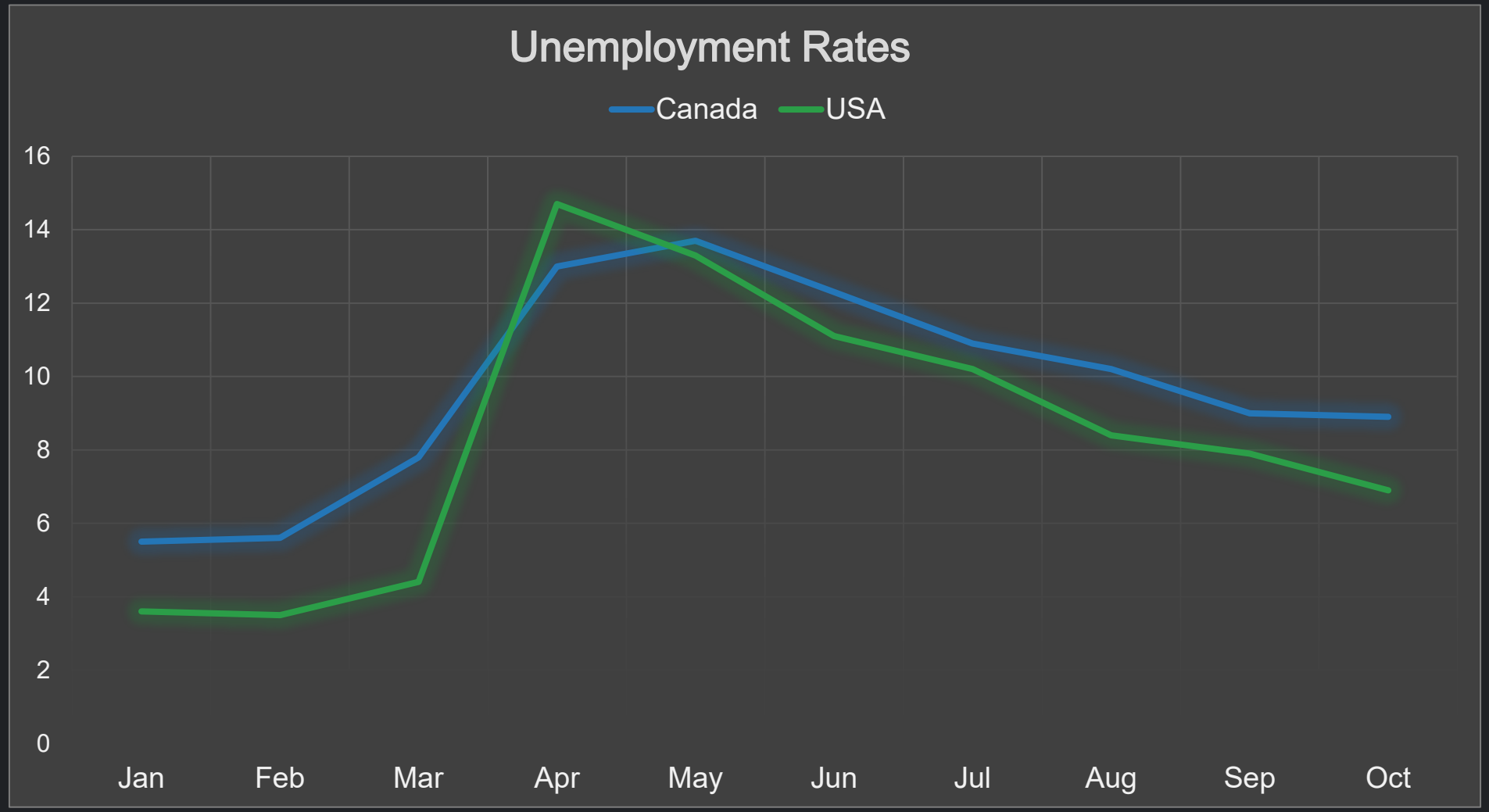
BEIJING – China is investigating an outbreak of atypical pneumonia that is suspected of being linked to severe acute respiratory syndrome (SARS), the flu-like virus that killed hundreds of people in the early 2000s, state media reported Tuesday.

A team of experts from the National Health Commission were dispatched Tuesday to Wuhan, in central China's Hubei province, and are "currently conducting relevant inspection and verification work," state broadcaster CCTV reported.

An emergency notification issued Monday by the Wuhan Municipal Health Committee said hospitals

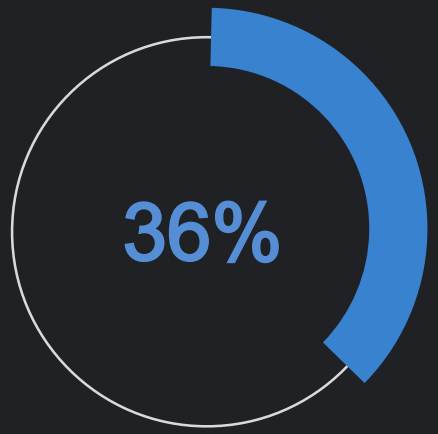
The New Insider Threat

THE NEW UNEMPLOYED

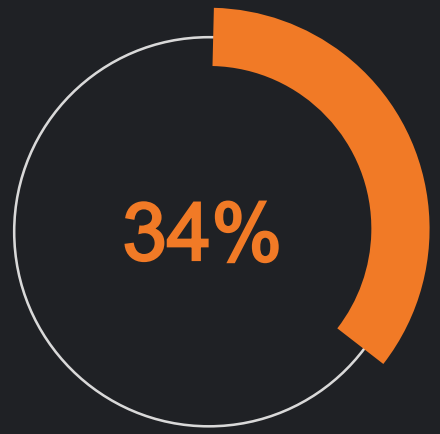


Source: Statistics Canada, Trading Econom

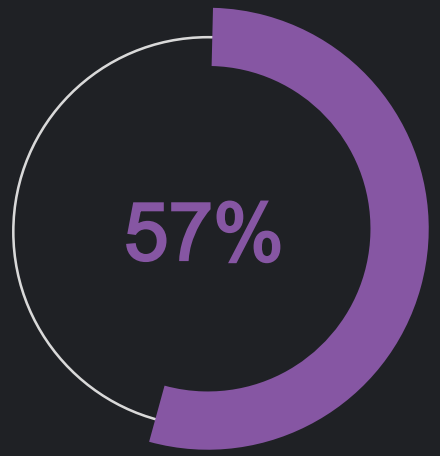
The New Freelancers



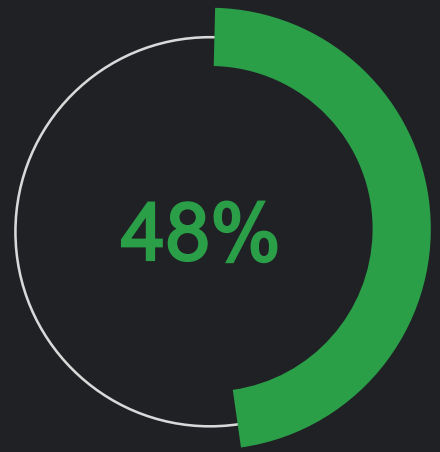
% of US Workers freelancing



% of freelancers who started due to pandemic



% of new freelancers providing skilled services

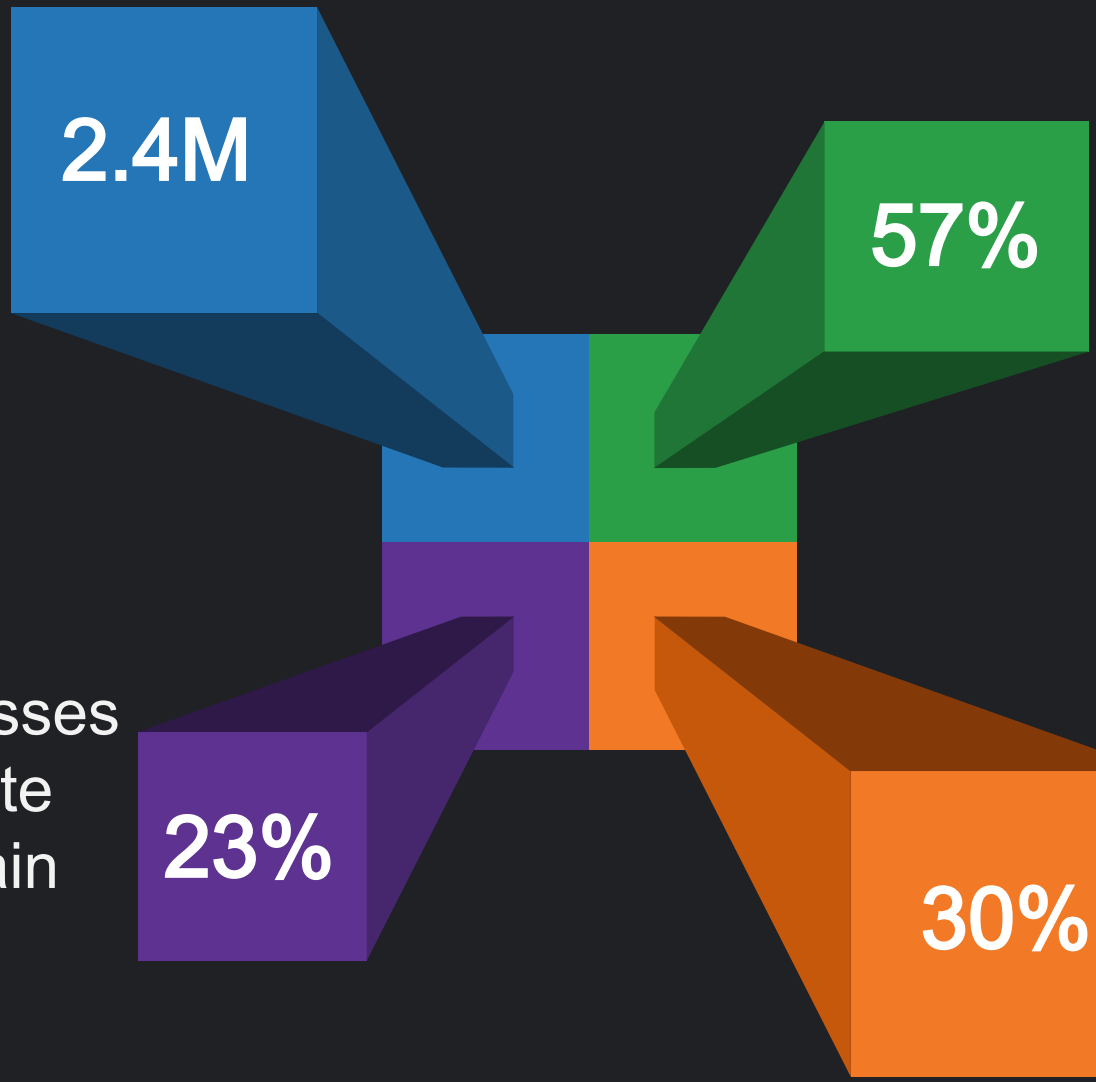


% of new freelancers who see freelancing as a long-term solution

Source: Upwork

The New Remote Work Normal

More Canadians working from home in October 2020 vs 2019



Businesses that do not include remote work risks in their security awareness program

Canadian businesses that expect remote working will remain normal post - pandemic

Security incidents caused by insider threats

Source: Statistics Canada, Ponemon, Verizon

The New Insider Threat

Economic Downturn

Resulting in layoffs and inability to hire new full-time staff.

Remote Workforce

Resulting in staff who are no longer within the security perimeter.

Corporate Gig Economy

Resulting in influx of new, untrusted freelancers to corporate workforce.

Ineffective Awareness

Resulting in a need to re-think security awareness for a remote workforce.

The End of Endpoint Protection

The Old Normal

- MALICIOUS CODE PROTECTION
- USER BEHAVIOR MONITORING
- DATA LOSS PREVENTION
- MANAGED RESPONSE

- HOST-BASED IDS/IPS
- PATCH MANAGEMENT
- APPLICATION CONTROL
- CONFIGURATION MANAGEMENT

The Old Normal

$12 Billion USD

Global endpoint protection market in 2019

Source: Fortune Business Insight

Endpoints in the New Normal

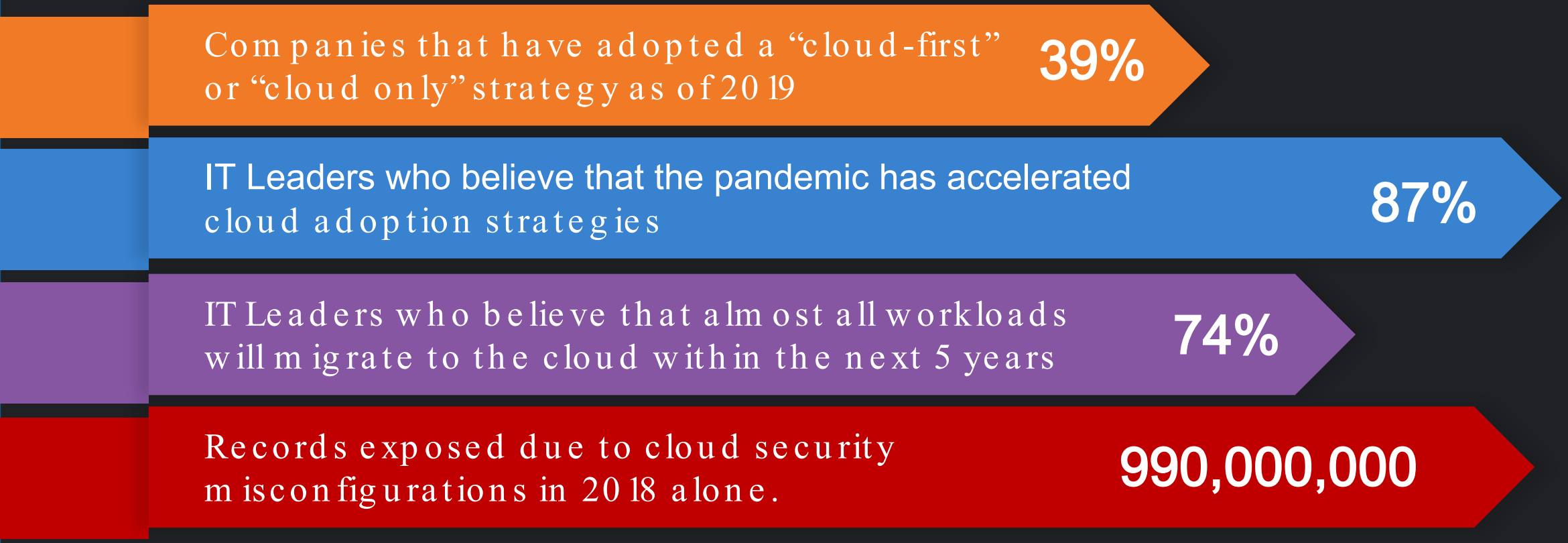
Rush to enable work-from-home forced many organizations to accept BYOD

Adoption of permanent remote workforce likely to also make BYOD permanent

Slow death of VPN removes ability to enforce even basic endpoint security controls

Data Centers without Data

The Dark Cloud Around the Silver Lining



Source: LogicMonitor, IBM

Data in the New Normal

Accelerated Cloud Adoption

Data not protected by IT Security

Accelerated BYOD

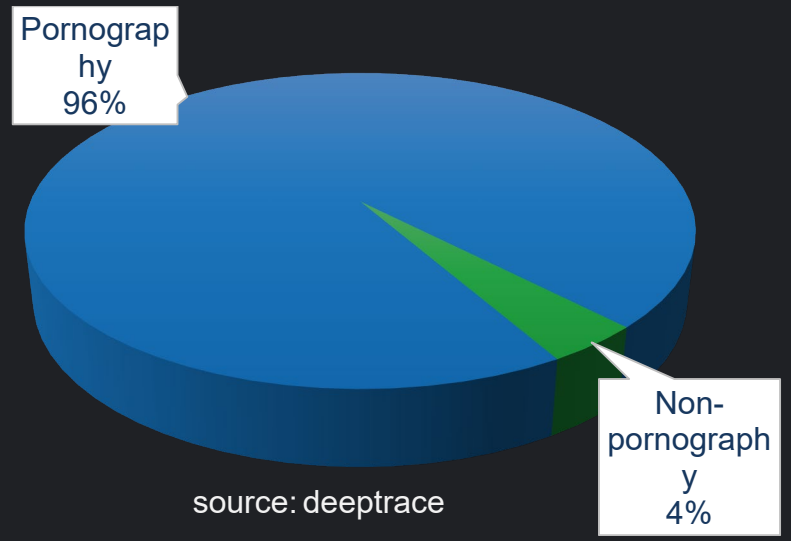
Data accessed by untrusted devices

Accelerated Remote Work

Data accessed by untrusted people

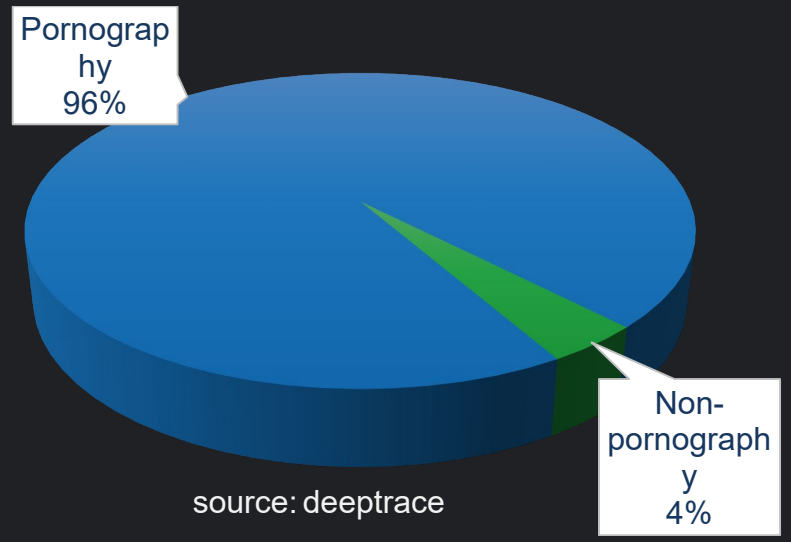
Wildcard Threat: Deepfake and Video Conferencing

96% of all online deepfake videos are pornographic in nature



source: deeptrace

96% of all online deepfake videos are pornographic in nature



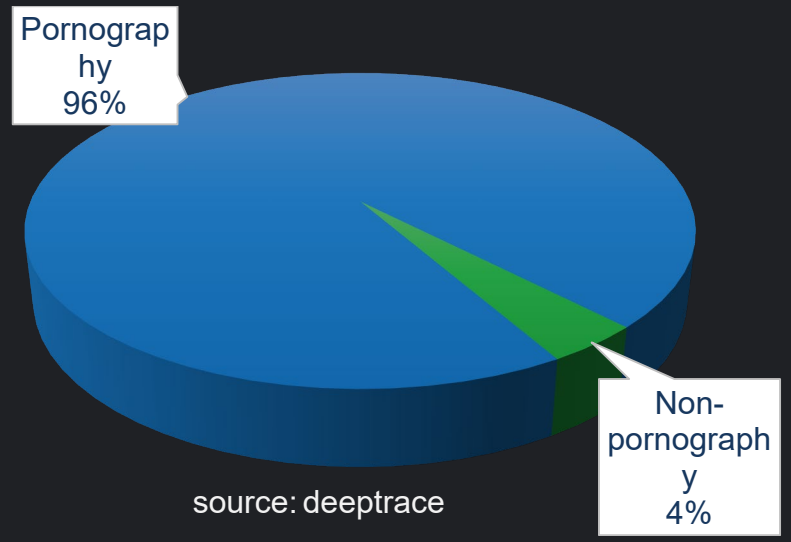
source: deeptrace

$243,000

amount stolen using synthetic voice audio in one 2019 incident

source deeptrace

96% of all online deepfake videos are pornographic in nature



source: deeptrace

$243,000

amount stolen using synthetic voice audio in one 2019 incident

source deeptrace

$68,000,000

spent by US defense on deepfake detection technology in 2018

source futurism.com

$10,000,000

contributed by Facebook for the 'Deepfake Detection Challenge'

source: facebook

Recommendations

Identify Internal Strategies

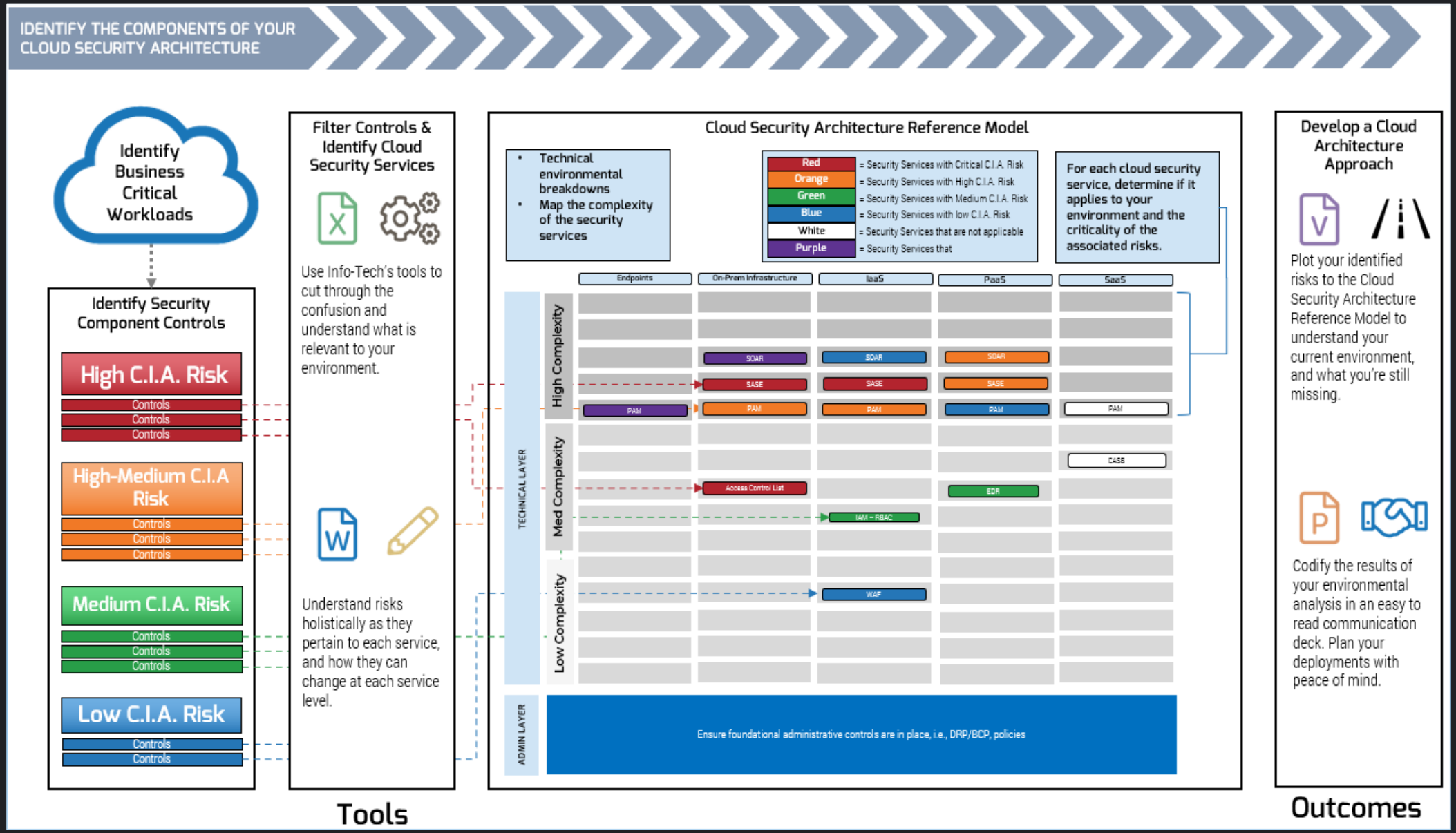
PLANS FOR USE OF FREELANCERS

REMOTE WORK STRATEGIES

BYOD STRATEGIES

CLOUD ADOPTION PLANS

Build a Cloud Security Architecture



Create a Data-Centric Security Strategy

Update Your Security Awareness Program

- FOCUS ON DATA SECURITY
- REMOTE WORK RISK TRAINING
- DEEPFAKE AWARENESS

Thank you!

Questions?

kpeuhkurinen@infotech.com

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

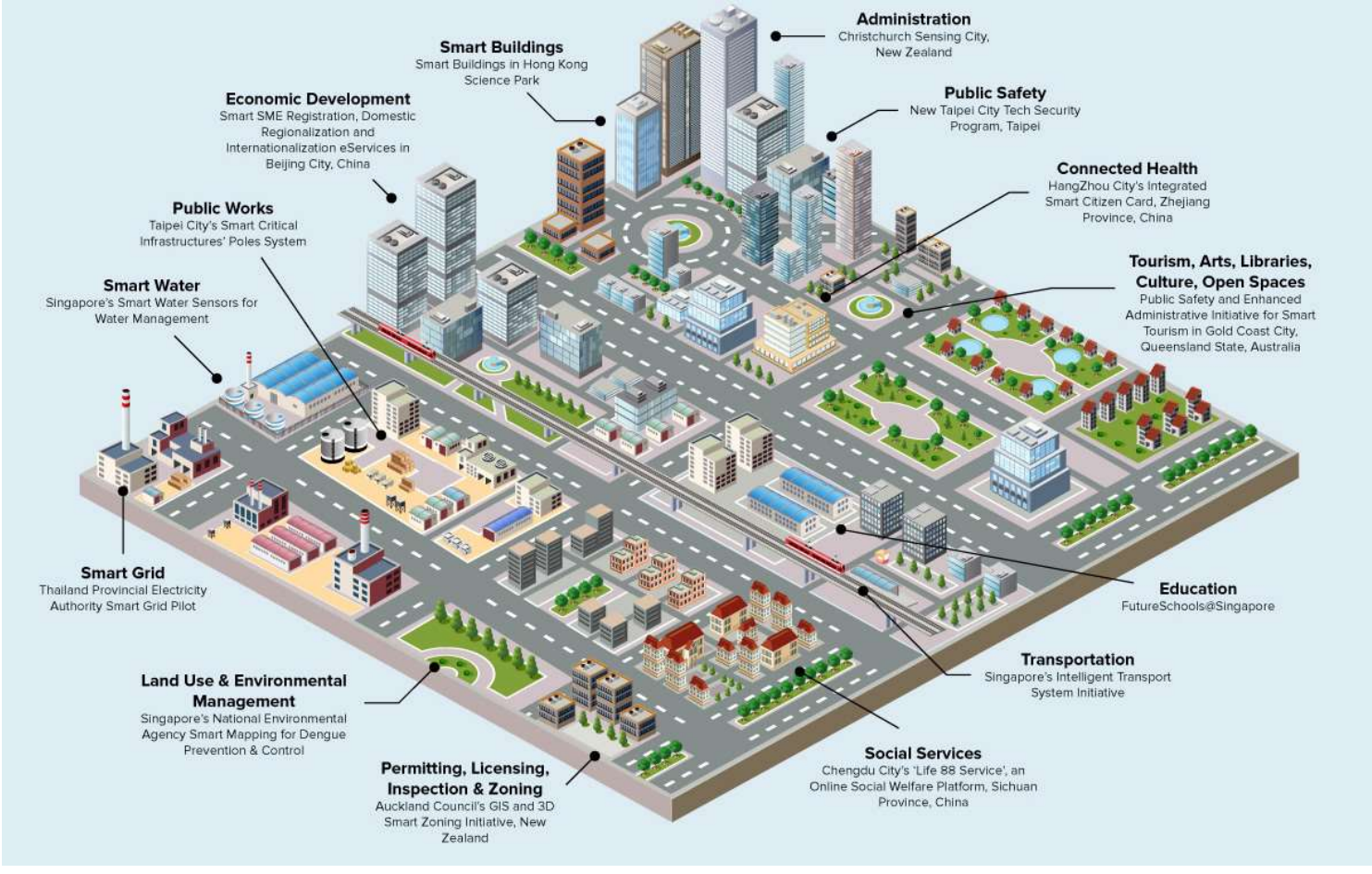
LA VILLE PROACTIVE INTELLIGENTE ET LES NOUVEAUX USAGES VERS UNE EXPÉRIENCE HUMAINE CONNECTÉE RÉSILIENTE

FRANÇOIS BÉDARD
Conseiller sénior innovation, stratégie et commercialisation

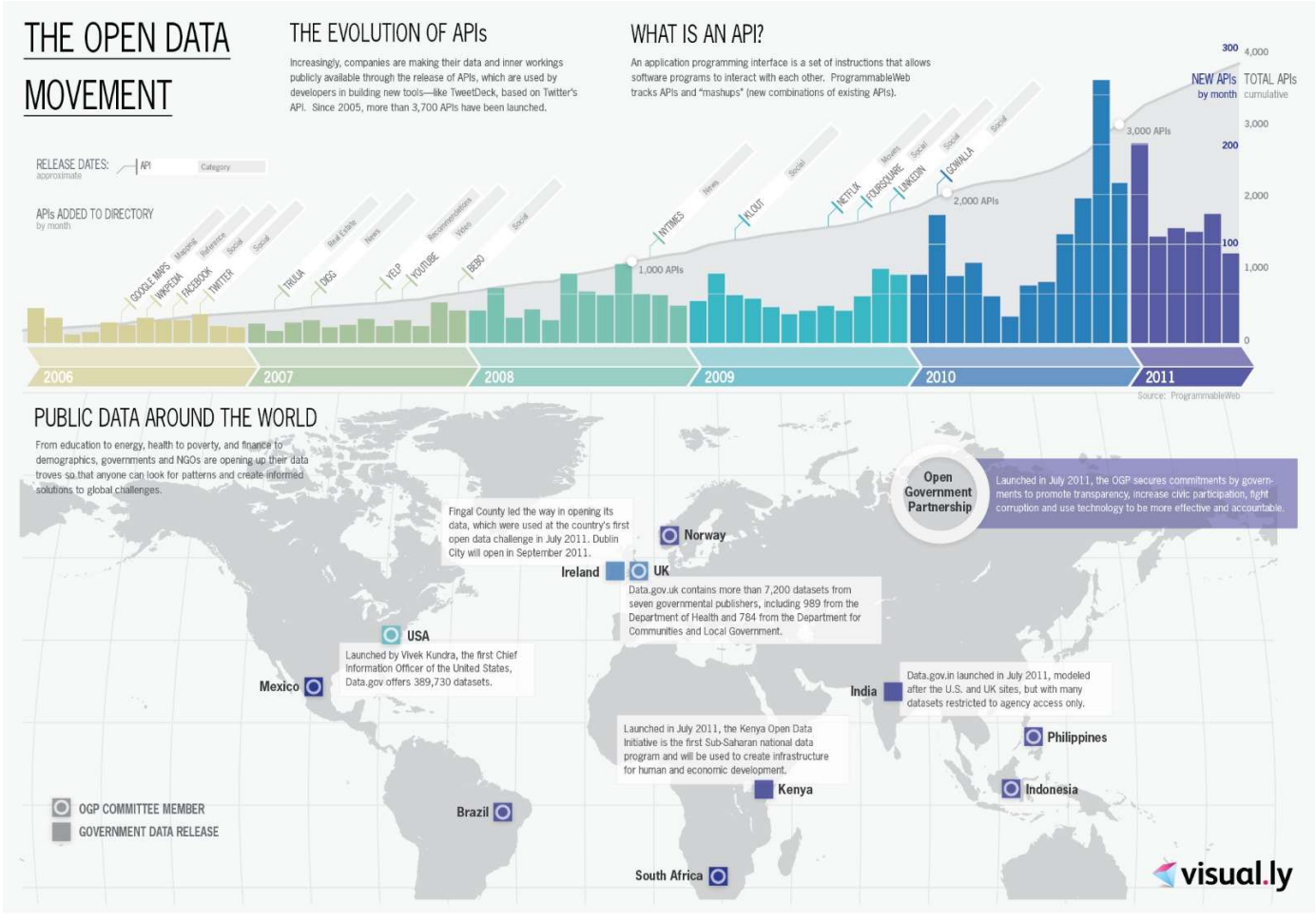
DIACC

CONFÉRENCE CYBER SÉCURITÉ 2020
ÉDITION VIRTUELLE

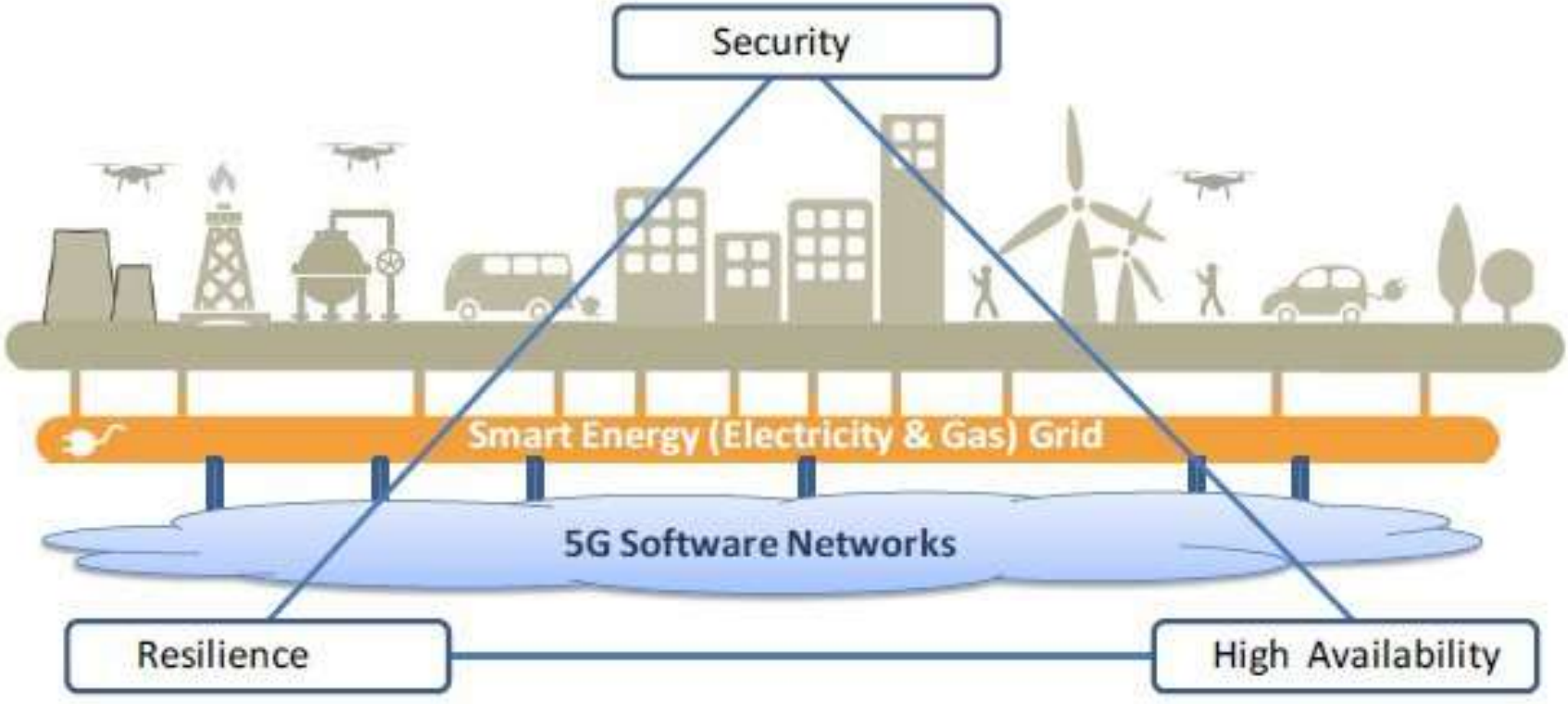
Smart Municipalites & more



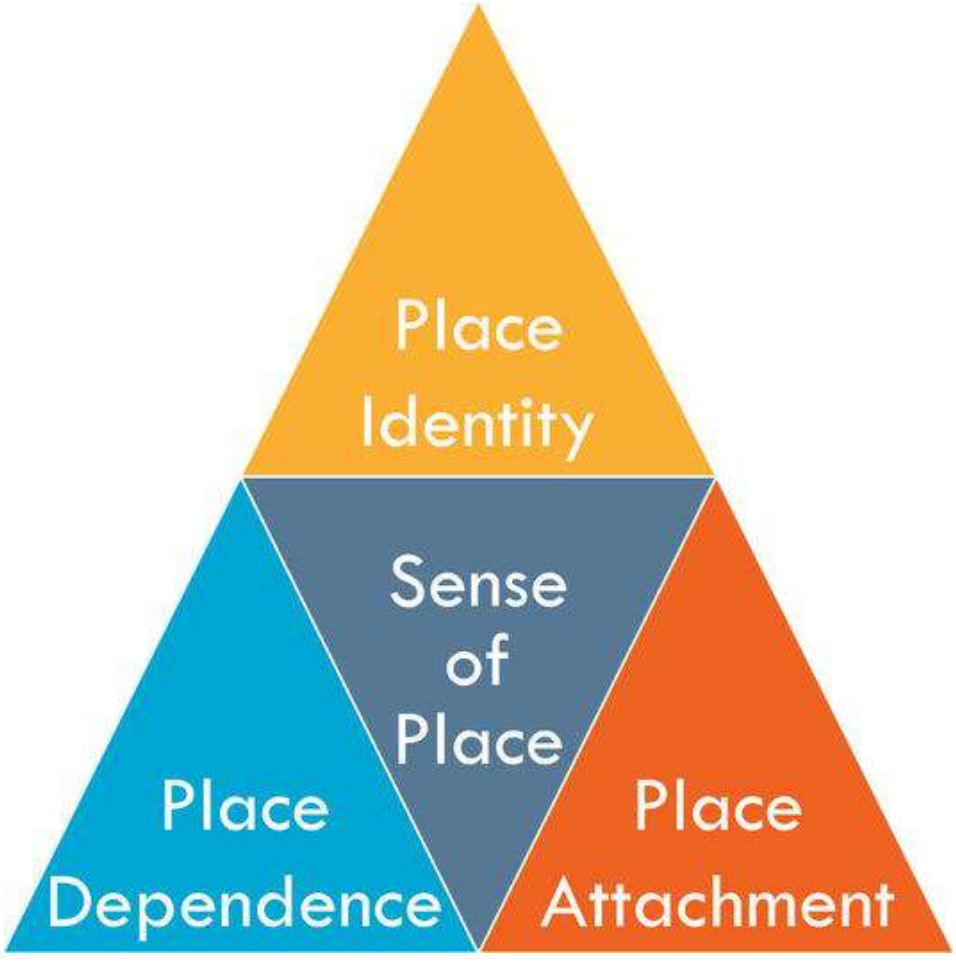
Smart Municipalites & more



Smart Municipalites & more



Smart Municipalites & more



Smart Municipalities highlights the urgent need for Canada to become a leader **of digital identity with a citizen focus**.

DIACC

What do Canadians think about smart cities?

Canadians' Perspectives on Smart Cities and Privacy

88%

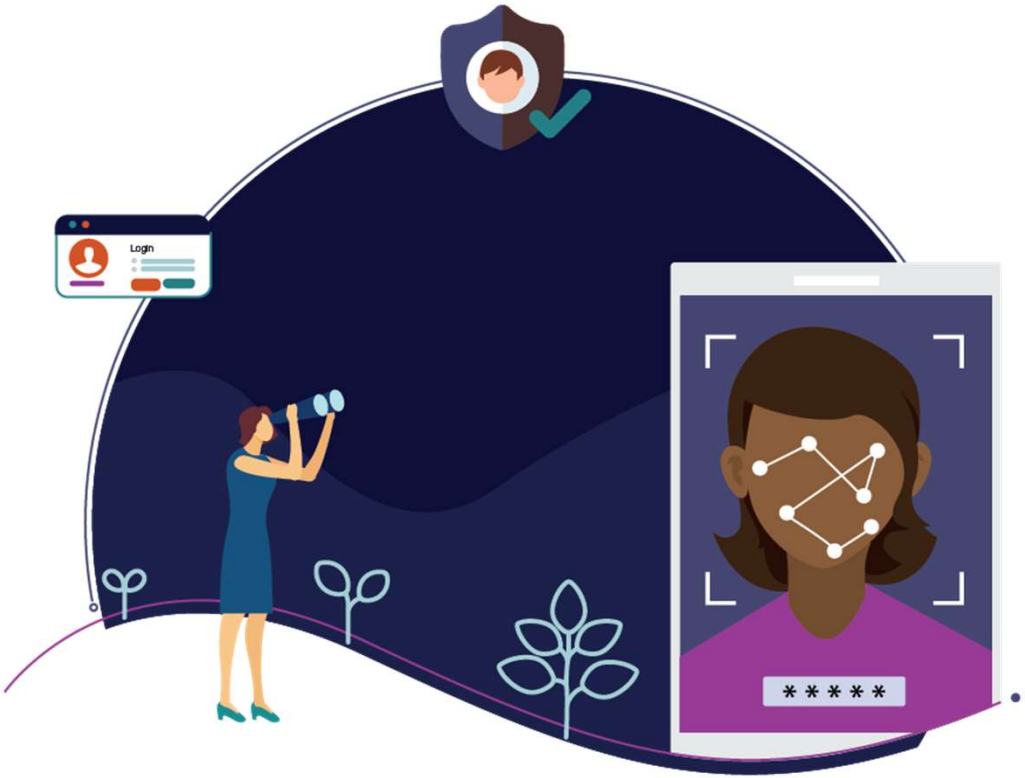
Concerned at some level about their privacy in the context of smart cities.

72%

For-profit sale of personal data related to smart cities should be prohibited.

DIACC

Source: https://smartcityprivacy.ca/survey-results/



How can concerns be addressed to ensure that smart cities respect residents?

Digital Identity
is a foundation of digital transformation

Canadians need to know what **data** exists **about them**

Citizens, governments, & businesses need **tools to manage sharing**

DIACC

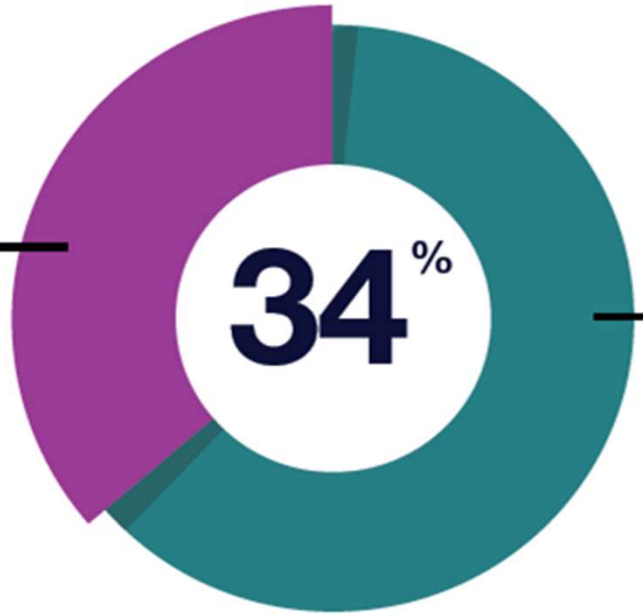
Digital Identity
done right has huge socioeconomic benefits.

Source: McKinsey & Co https://www.mckinsey.com/featured-insights/innovation-and-growth/the-value-of-digital-id-for-the-global-economy-and-society

What do Canadians think about digital identity?

Canadians' Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**



compared to ~4-in-5

83% trusting the government

81% trusting financial institutions

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

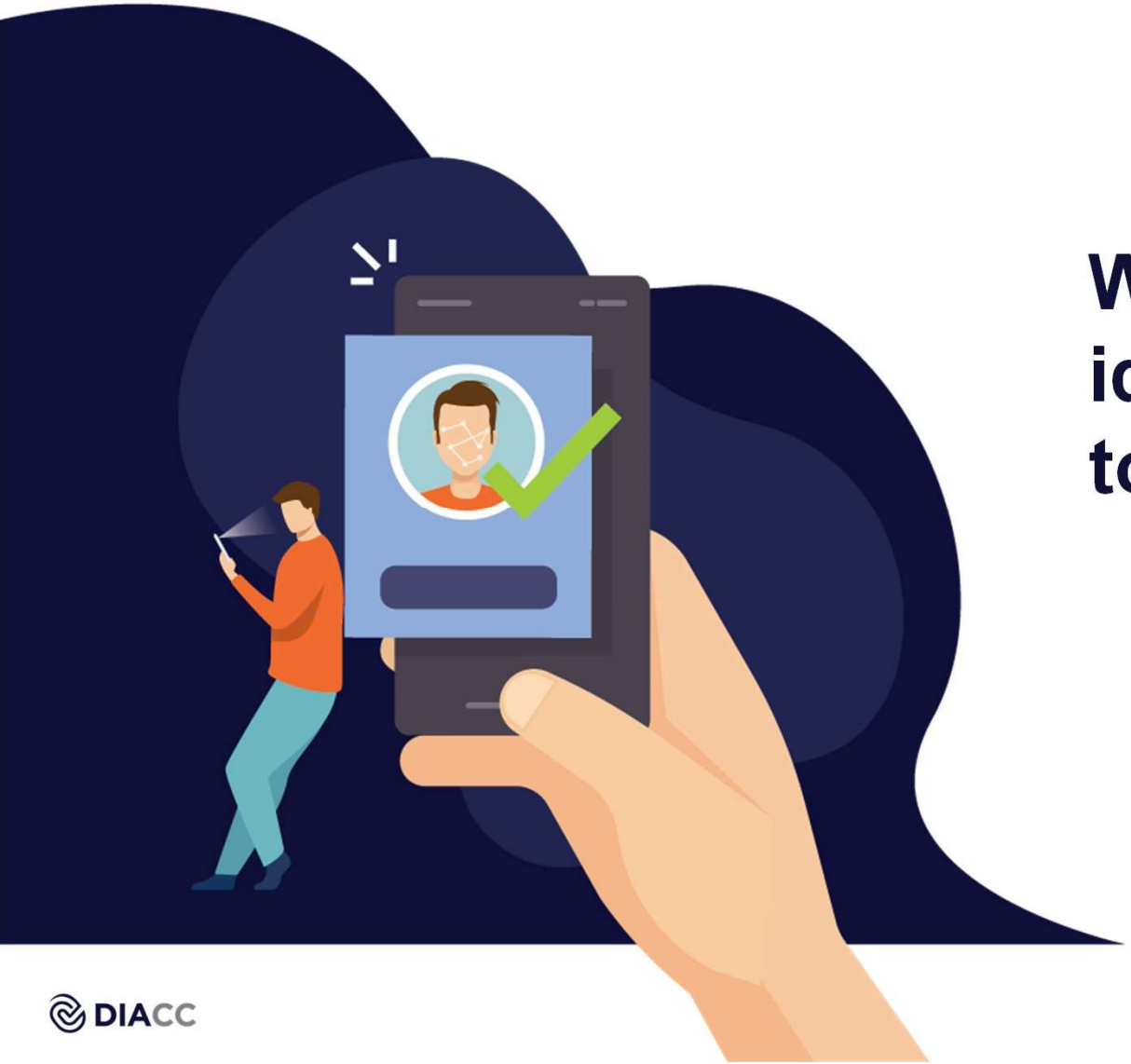
Canadians' Perspectives on Digital Identity

70%

feel that a collaboration between the government and the private sector is the **best approach to creating a pan-Canadian digital ID framework**.

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/



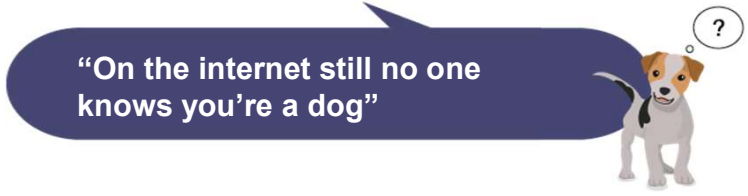
What does digital identity look like today?

On the internet, nobody knows you’re a dog

Possible future scenarios

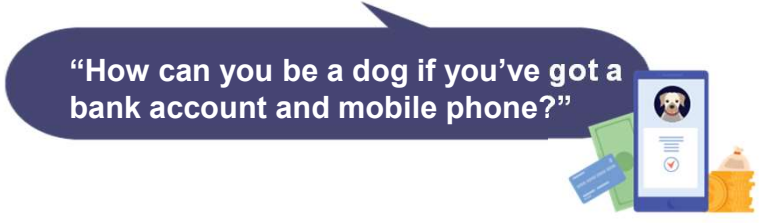
Platform Identity

The internet giants have tried to adapt their business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.



Operator Networks

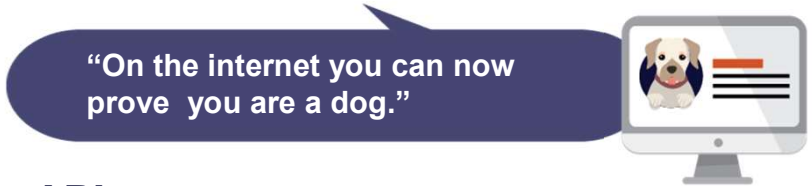
To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but does help in those services where identity matters the most.



Possible future scenarios

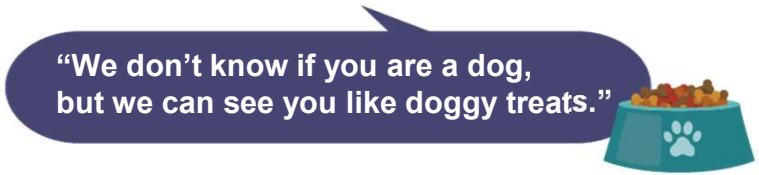
Self-Sovereign Identity

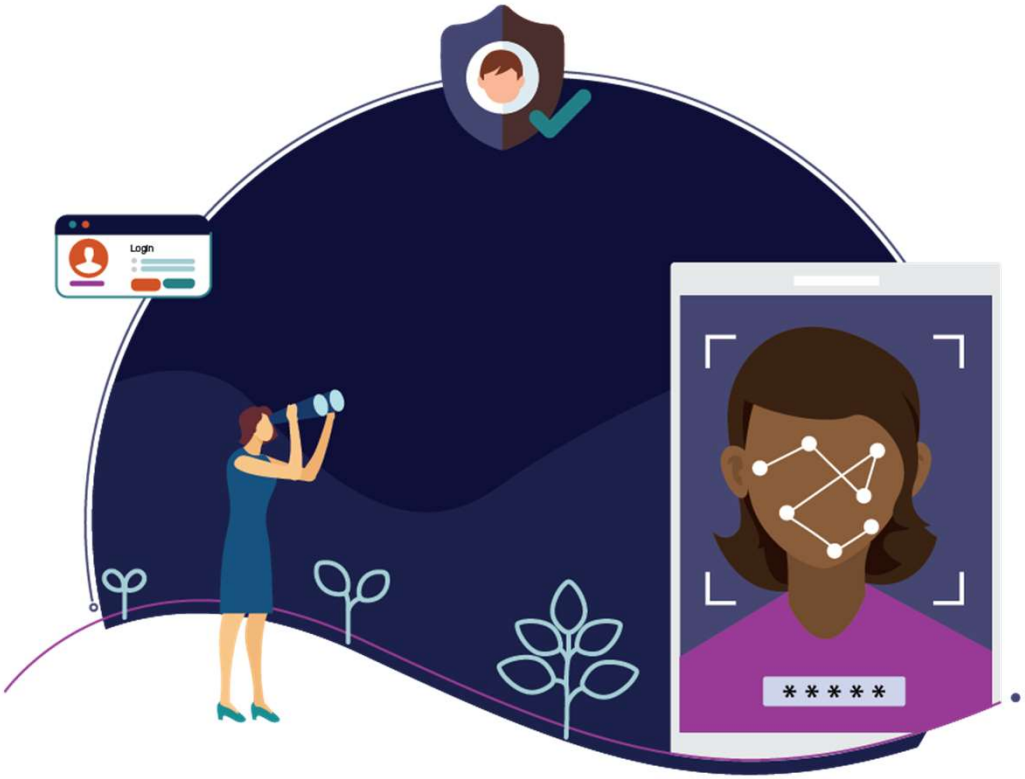
Users and businesses have begun to realize a need to fundamentally change the way personal data is managed. For businesses, personal data is a liability due to data protection risks. Users see the value of being able to hold data and take it where they need it. For this to work, data presented by users needs to be reliable and trustworthy. Some have started to use cryptographic wallets to collect and share signed data. Users need to look after their data, much like they look after their money.



Open APIs

Identity networks never really took off, due to a combination of users not really understanding what digital identity is and organizations not appreciating the longer-term business benefits. Organizations across the economy have been forced to open APIs allowing services to access user data (with the user’s consent) from other places. Users link together different services as the need arises. It is down to the individual service to piece together all the data it collects into something meaningful for the particular user. Most individual users don’t remember all the connections and links they have set up.





How do we ensure that identity will respect citizens and consumers?

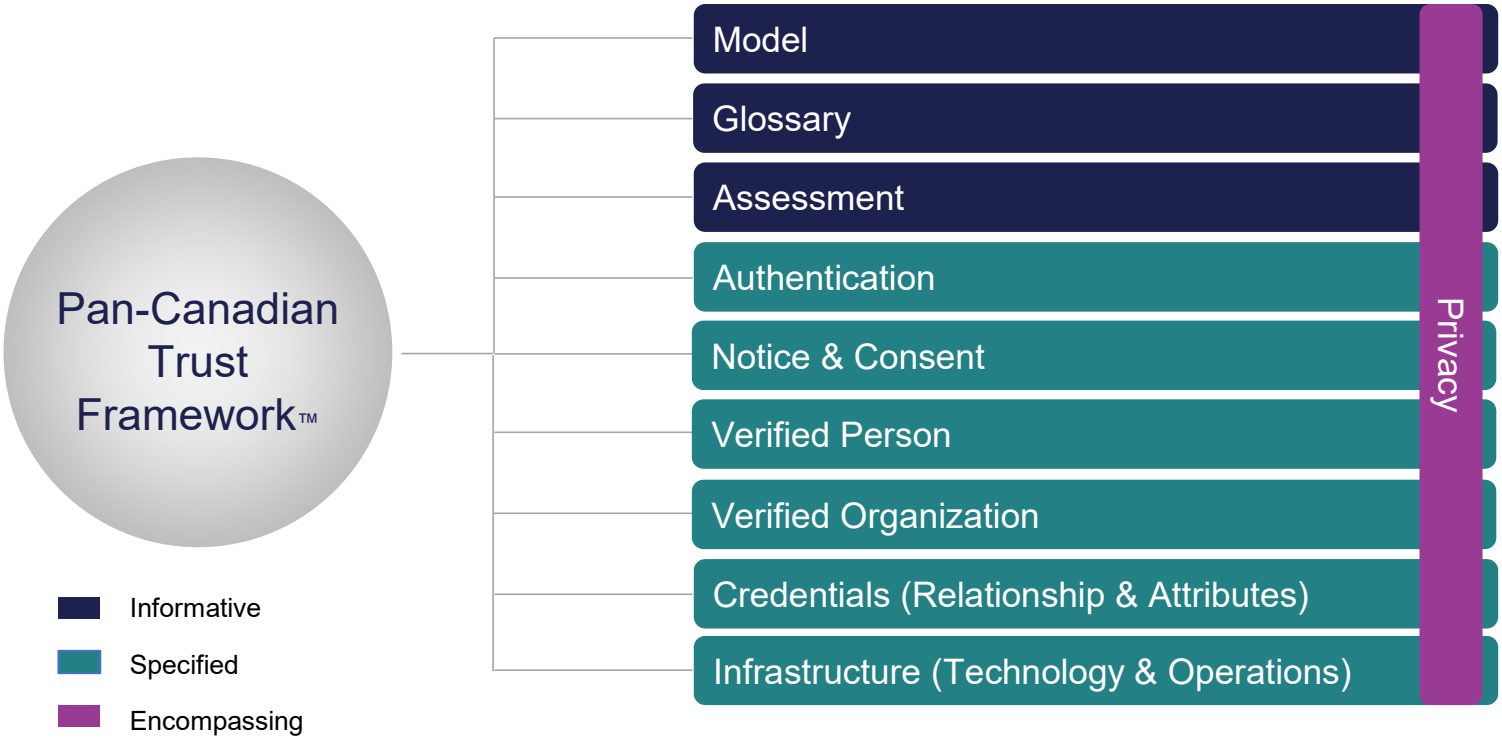
One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.

Led by the DIACC with **multi-sectoral pan-Canadian and international input**, the PCTF is connecting and enabling Canada's digital economy from coast-to-coast-to-coast.

Developed to secure **cross-sector identity interoperability** with a focus on industry standards and practices. PCTF is available @ **DIACC.ca**

A Pan-Canadian Trust Framework for Digital Services



A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More


DIACC
Strong collaboration and leadership in Digital Identity is vital to Canada's economic and societal success.

The Digital ID & Authentication Council of Canada

Leading Canada's **full and beneficial global digital economy participation** by delivering a **digital identity and authentication interoperability framework.**

The DIACC is a **Non-profit coalition** of **public and private sector members** created as a result of federal government's Electronic Payments System Task Force.

DIACC Board of Directors

Government of Canada

Sustaining Members (Tier 3)

Sustaining Members (Tier 2)

Sustaining Members (Tier 1)

DIACC Strategic Goals

Accelerate

Interoperability through public and private sector adoption of the Pan-Canadian Trust Framework.

Develop

Develop and launch a certification program aligned with market needs.

Publish

The Pan-Canadian Trust Framework and identify legislative needs to support the vision.

Raise

Canada's identity innovation profile via DIACC as Canada's identity forum.

Create

Canadian expertise and intellectual property for excellence in identity.

Join the Conversation!

Adopt the Pan-Canadian Trust Framework to secure the foundation of digital identity that will enable innovative smart cities to work for all.

Contact us to join the conversation info@diacc.ca

diacc.ca @mydiacc /company/mydiacc /mydiacc

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

LA FACILITÉ DE PIRATER UNE ENTREPRISE – D'UNE RECHERCHE GOOGLE À UNE BRÈCHE COMPLÈTE!

PATRICK R. MATHIEU
Cofondateur, Hackfest.ca

CONFÉRENCE
CYBER
SÉCURITÉ
2020
ÉDITION VIRTUELLE

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

L'HISTOIRE D'UNE CYBERATTAQUE VUE DE L'INTÉRIEUR – TÉMOIGNAGE ANONYME

JOHN DOE
Directeur informatique
Entreprise anonyme

CONFÉRENCE CYBER SÉCURITÉ 2020
ÉDITION VIRTUELLE

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

SALLE DE GESTION DE CRISE, RÔLES ET ANIMATION

PASCAL PARENT
Président de PMU Québec

CONFÉRENCE CYBER SÉCURITÉ 2020 ÉDITION VIRTUELLE

PMU QUÉBEC

P.M.U.
QUÉBEC

Salle de gestion de crise, rôles et animation

PMU Québec ?

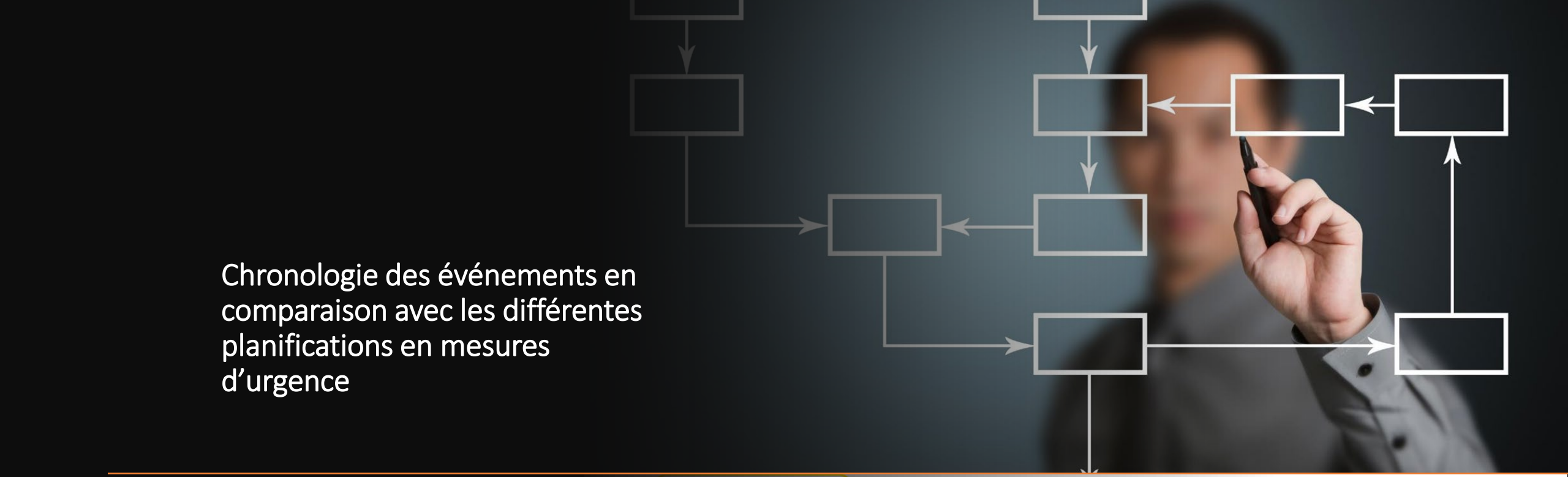
- Leader en mesures d'urgence au Québec (2007).
- Projets majeurs dans notre domaine.
- 2000 plans d'urgence à ce jour.
- Une équipe dédiée et reconnue dans notre milieu.
- Récipiendaire de trois triangles de l'ATPIQ.
- Membres: ASCQ, ATPIQ, CRAIM, RÉCO-Québec, SFPE,etc.
- www.pmuquebec.com
- Info@pmuquebec.com
- Tel ; 450-845-3366

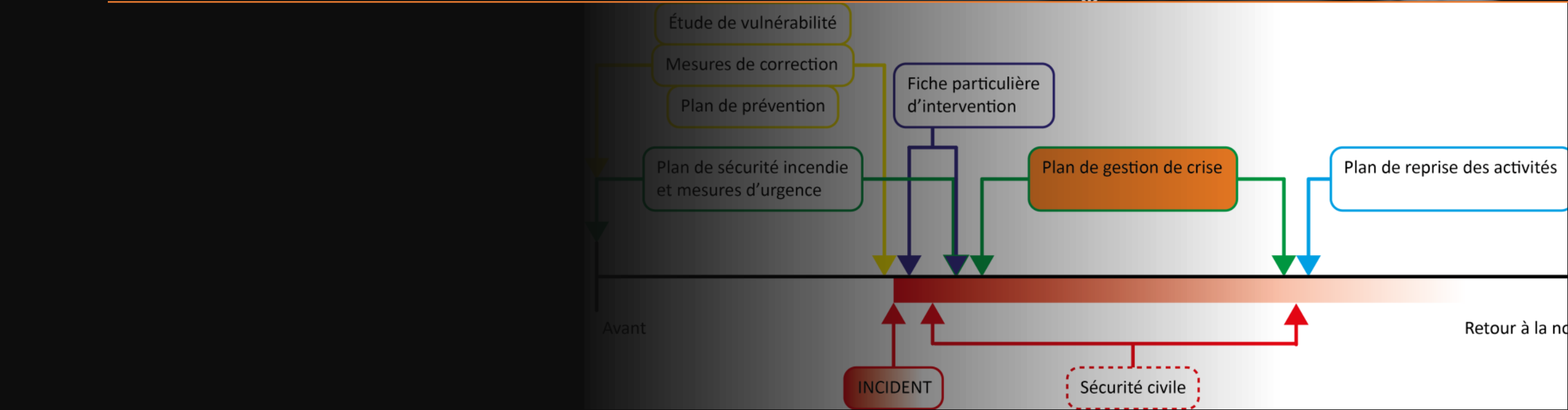
- Pascal Parent (LinkedIn)

1- Introduction – Gestion de crise

- Le plan de gestion de crise doit être mis en œuvre lors de situations majeures, notamment lorsqu'il est question :
  - De la sécurité, de la protection des biens ou de l'environnement.
  - De l'évacuation lieux advenant une intervention d'urgence.
  - Des enjeux politiques ou communautaires.
  - De l'attaque de l'image de marque.

Chronologie des événements en comparaison avec les différentes planifications en mesures d'urgence





2. Organisation
Gestion de crise

CYBERATTAQUES RÉPERTORIÉES

chez les membres de la Mutuelle des municipalités du Québec

2012 VILLE D'ALMA	2016 VILLE DE BAIE-ST-PAUL
2012 VILLE DE SUTTON	2018 MRC DE MÉKINAC
2014 MRC DE TÉMISCAMINGUE	2018 MUNICIPALITÉ DE CHERSTEY
2015 TERRASSE-VAUDREUIL	2018 FOSSAMBAULT-SUR-LE-LAC
2015 VILLE DE LA MALBAIE	

SOURCE : MUTUELLE DES MUNICIPALITÉS DU QUÉBEC

2.1 Le comité de gestion de crise

- Confirme la situation à la division corporative (s’il y a lieu).
- Précise les objectifs dans l’ordre des priorités.
- Maximise le passage de la crise vers l’urgence.
- Prend des décisions.
- Envisage les mesures possibles et probables selon le temps.
- Assure des communications efficaces avec toutes les parties concernées en priorisant d'abord le milieu local.
- Donne des conseils aux équipes d’intervention et leur offre du soutien dans certains cas.
- Facilite la reprise des opérations (PCO)

3. Mode décisionnel

- Vote 50%+1
- Unanimité
- Directeur ayant un droit de véto

4. Identifier les rôles

Les rôles doivent être occupés par des fonctions ou des personnes qui connaissent les différents départements de l'entreprise.

- **Directeur comité de gestion de crise (adjoint)**
- **Communications (employés, réseaux sociaux, etc.)**
- **Responsable SST**
- **Sécurité**
- **Environnement**
- **Logistique**
- **Techniques informatique**
- **Tenue de registres**
- **Administration**

- *Aide aux sinistrés (OSBL)*
- *Conseillers invités*
- *Photographe*
- *Services d'urgence*
- *(lien) coordonnateur MU*
- *Météorologues*
- *Chef décontamination*
- *Agence gouvernementale (OMSC)*
- *Autres….*

Quand ouvrir le comité de gestion de crise?

- Il est souhaité d'analyser les ALÉAS de votre entreprise.
- Se baser sur votre étude de vulnérabilité.
- Vaux mieux ouvrir un peu qu'en retard.

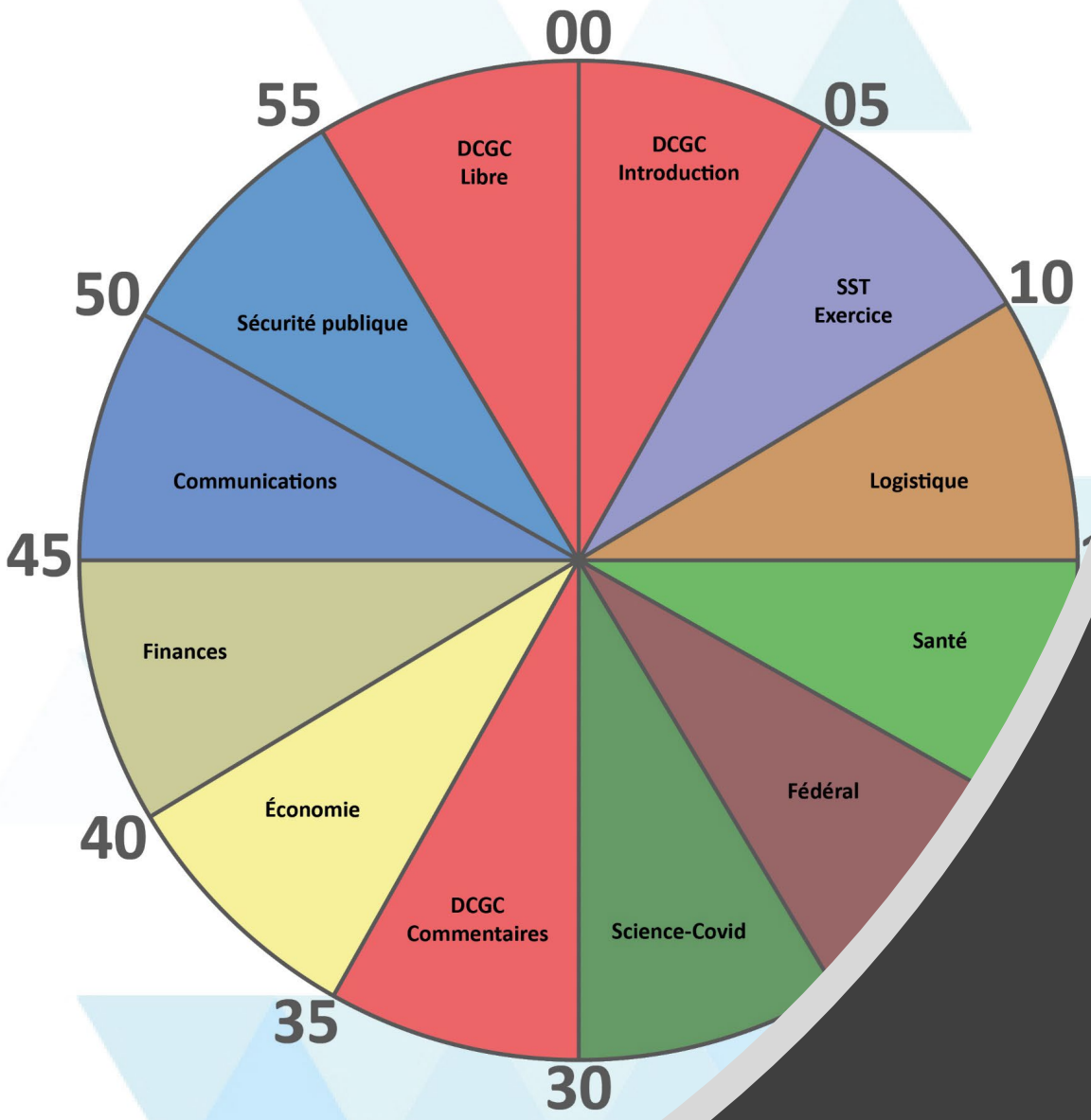
Incident	Ouverture Plan de gestion de crise
Accident d'aéronef	Oui
Accident grave	Oui sur demande du coordonnateur MU
Accident avec radioactivité	Oui sur demande du coordonnateur MU
Alerte à la bombe	Oui sur demande du coordonnateur MU
Bris de digue	Sur demande
Effondrement d'une structure de bâtiment	Oui sur demande du coordonnateur MU ou DO
Évacuation – Bâtiment	Oui sur demande du coordonnateur MU
Évacuation – Générale	Oui
Évacuation –	Oui sur demande du coordonnateur MU ou DO
Désobéissance civile	Oui sur demande du coordonnateur MU
Déversement de matières dangereuses	Oui sur demande du coordonnateur MU
Déversement de matières dangereuses (HCL)	Oui sur demande du coordonnateur MU
Incendie - Général	Oui sur demande du coordonnateur MU
Incendie – Avec explosifs	Oui
Incendie – Feu de forêt	Oui sur demande du coordonnateur MU
Panne électrique	Oui sur demande du coordonnateur MU
Pandémie	Oui

Rassembler les faits

- Qu’est-ce qui fonctionne en ce moment?
- Demandez la confirmation de la compréhension des faits. (deux sources fiables).
- De quoi as-t ’on besoin?
- Prendre le temps d’établir vos priorités
- Demander conseils
- Soyez à l’écoute des autorités.

Surveillance et reprise des priorités

- Refaire constamment les priorités.
- Ne pas oublier que vous avez une famille et des amis.
- Revenez constamment à l’Humain , l’Environnement et le Bâtiment.
- Prévoyez la semaine prochaine.
- …Si la tendance se maintient….



6. Cadran de l'heure

- Exercice au début de l'ouverture
- 5 minutes par rôle.
- Pause décisionnelle et animation par le DCGC.
- 15 minutes de pause par heure.
- Décrire les priorités et les accomplissements.

Définir une manière de répondre avant de diffuser

- Ligne d’information 1-800 (fournisseur de service).
- Une adresse courriel.
- Interagir avec les demandes.
- Utiliser vos communiqués existants

Par volet M.S.G.U.
Médias sociaux en situation d'urgence

- Création de notification d'urgence.
- Facebook Urgence – employés (groupe secret).
- Twitter -urgence incluant un #hashtag
- Avis sur LinkedIn.

Service à la clientèle.

Formation et exercice

- Formation régulière et deux fois l'an aux personnes ayant un rôle dans le plan.
- Exercice de table.
- Pratique d'ouverture de la salle de gestion de crise.
- Pratique suivant l'exercice d'urgence annuelle de l'organisation.

Transition de la relève.

- Responsable SST et DCGC.
- 7 heures au centre de gestion de crise.
- Exercice physique à l’heure obligatoire.
- Une durée d'une heure est requise pour transférer des connaissances à notre remplaçant.

Fin de la crise

- En crise, on ne sait pas quoi faire, en urgence on sait quoi faire.
- Utiliser le terme URGENCE lorsque vous êtes en contrôle.
- Lorsque l’incident est terminé, on démarre le plan de reprise des activités.
- C’est le retour à la normal en fonction des dommages à l’organisation.
- Certains dommages peuvent être permanents

Des questions ?

- info@pmuquebec.com
- 450-845-3366

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

DIGITAL IDENTITY – A VISION FOR CANADIAN PROSPERITY AND INCLUSION

Digital ID and Authentication Council of Canada

JONI BRENNAN
Présidente
DIACC

DIACC

CYBER SECURITY CONFERENCE 2020 VIRTUAL EDITION

Source: McKinsey & Co https://www.mckinsey.com/featured-insights/innovation-and-growth/the-value-of-digital-id-for-the-global-economy-and-society

Digital Identity

Digital Identity
is a foundation of digital transformation

Canadians need to know what **data** exists **about them**

DIACC

Canadians need to know what **data** exists **about them**

Citizens, governments, & businesses need **tools to manage sharing**

DIACC


DIACC
What do Canadians think about digital identity?
DIACC

Canadians' Perspectives on Identity and Privacy

DIACC

Source: https://smartcityprivacy.ca/survey-results/

Canadians' Perspectives on Identity and Privacy

88% Concerned at some level about their privacy in the context of smart cities.

DIACC

Source: https://smartcityprivacy.ca/survey-results/

Canadians' Perspectives on Identity and Privacy

88% Concerned at some level about their privacy in the context of smart cities.

72% For-profit sale of personal data related to smart cities should be prohibited.

DIACC

Source: https://smartcityprivacy.ca/survey-results/

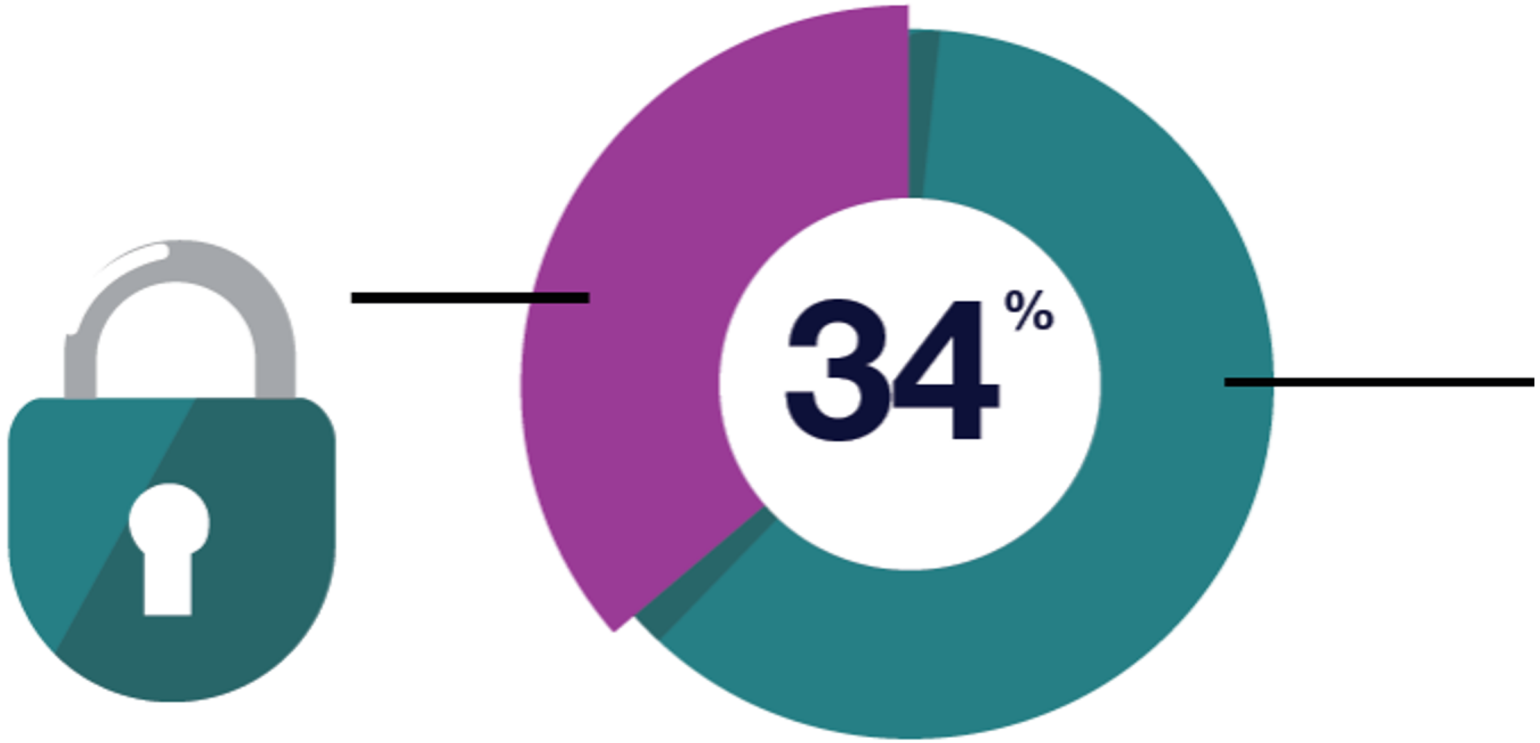
Canadians' Perspectives on Digital Identity

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians' Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**

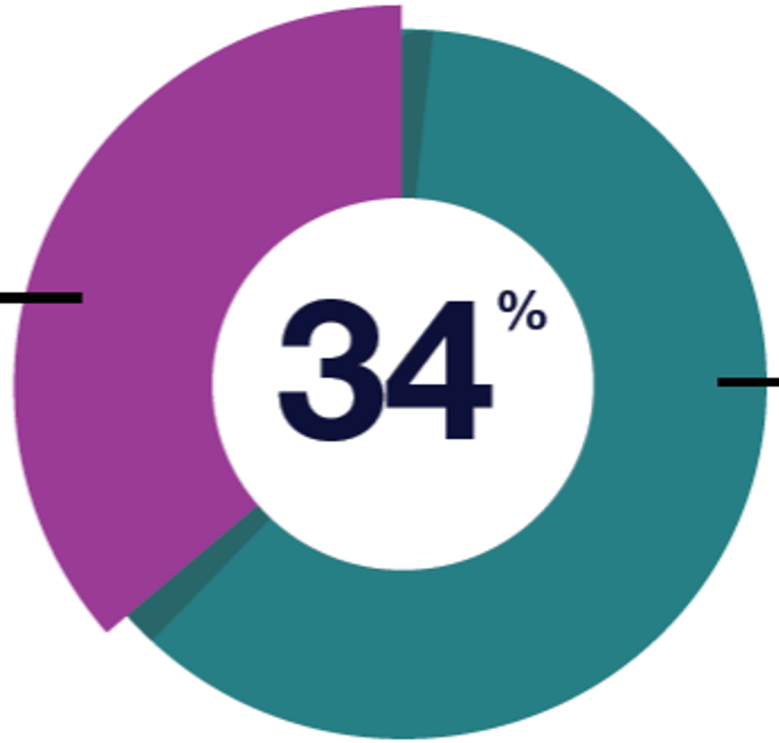


DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians' Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**



compared to ~4-in-5

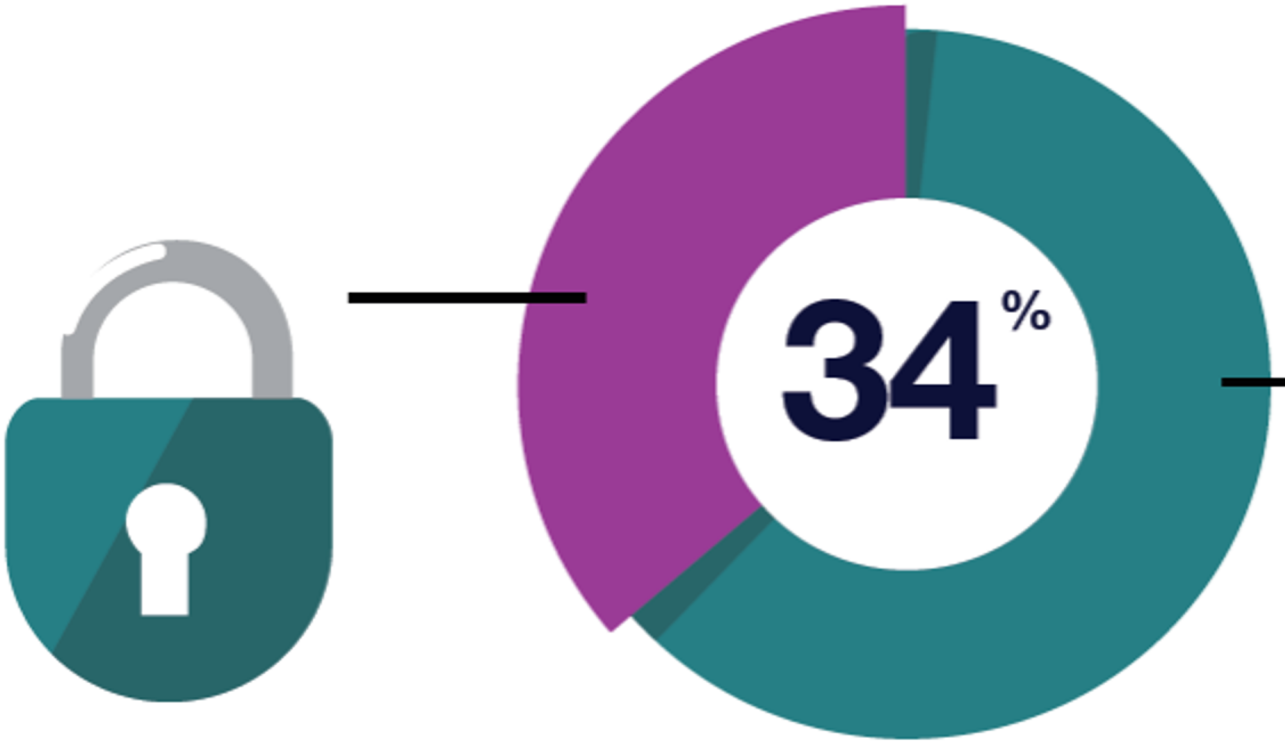
83% trusting the government

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians' Perspectives on Digital Identity

Canadians are concerned with how social media sites use their personal information; **Just one-third** trust social media sites to keep their personal information **safe and secure.**



compared to ~4-in-5

83% trusting the government

81% trusting financial institutions

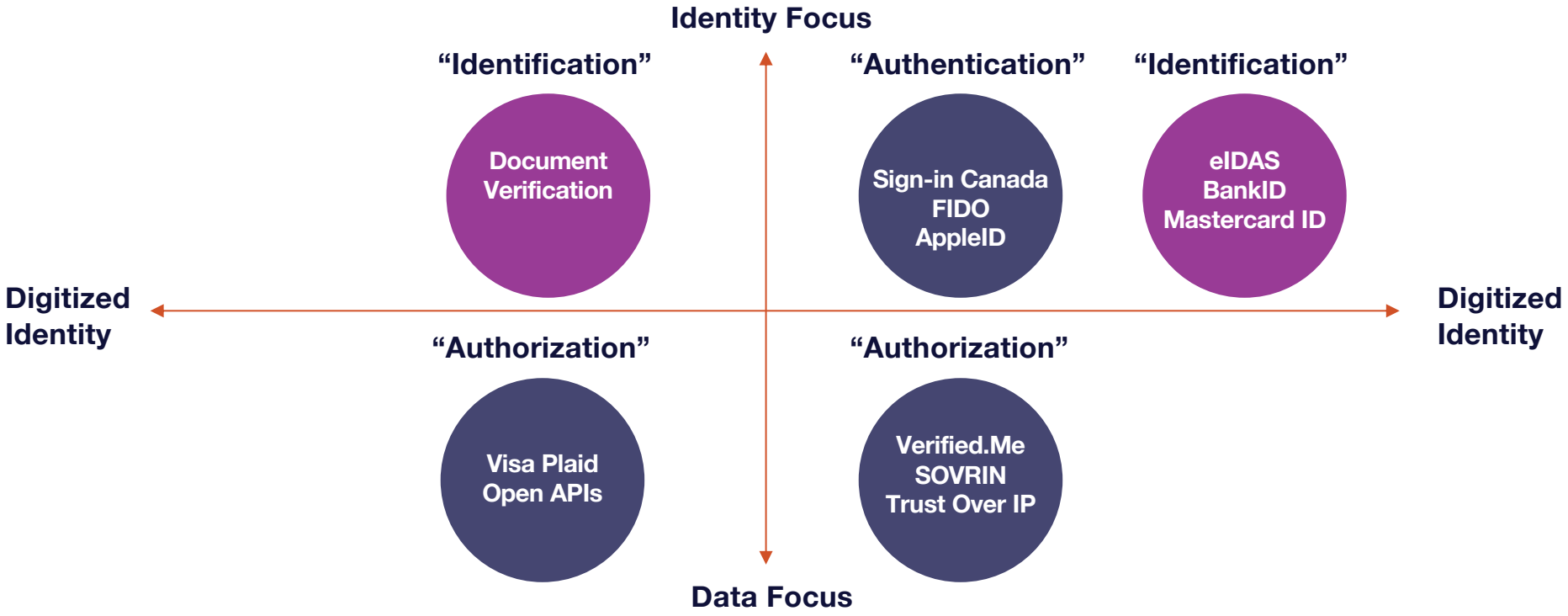
DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

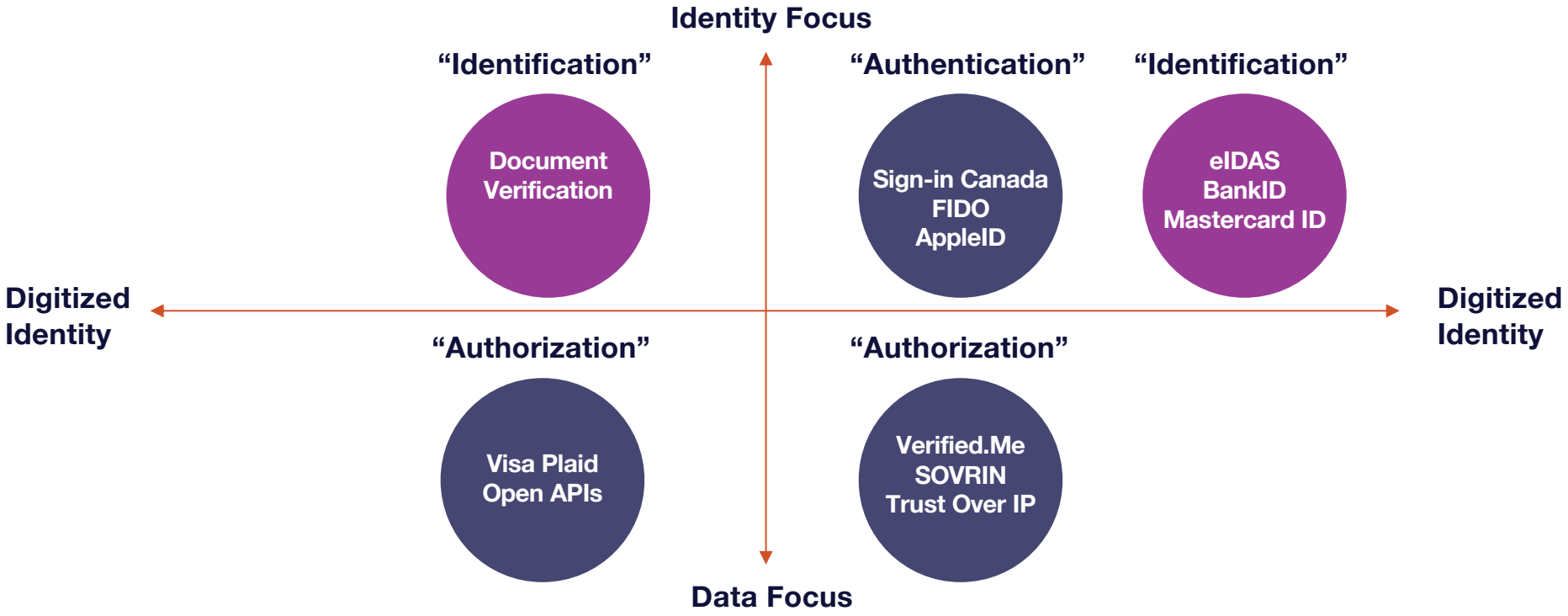
What does digital identity look like today?

DIACC

What does digital identity look like today?



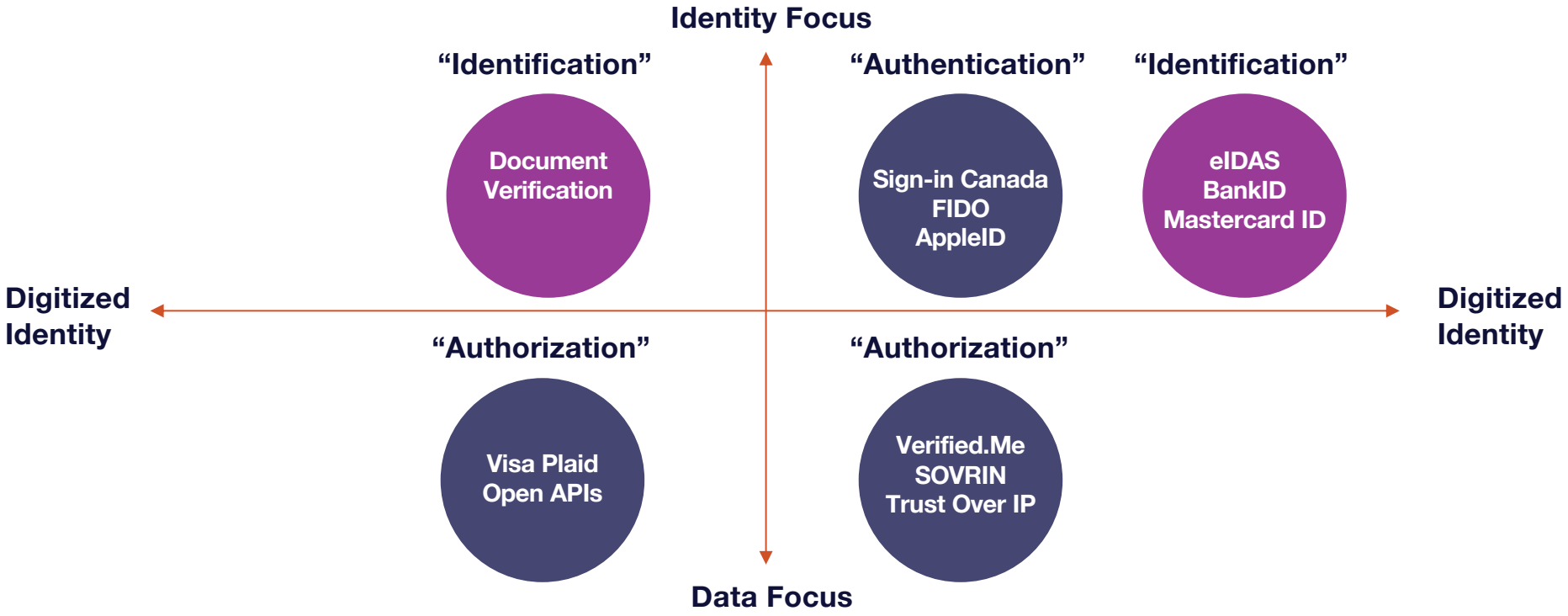
What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

What does digital identity look like today?



Theme: Identity vs Identification

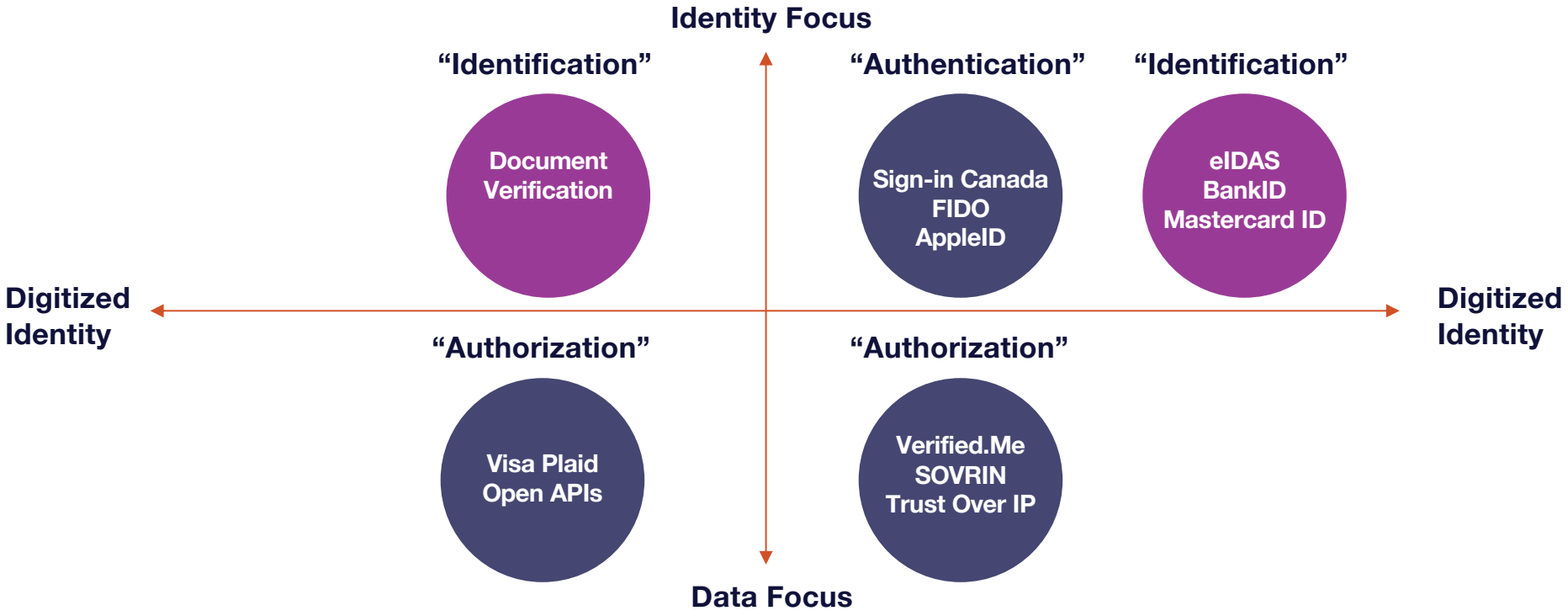
Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

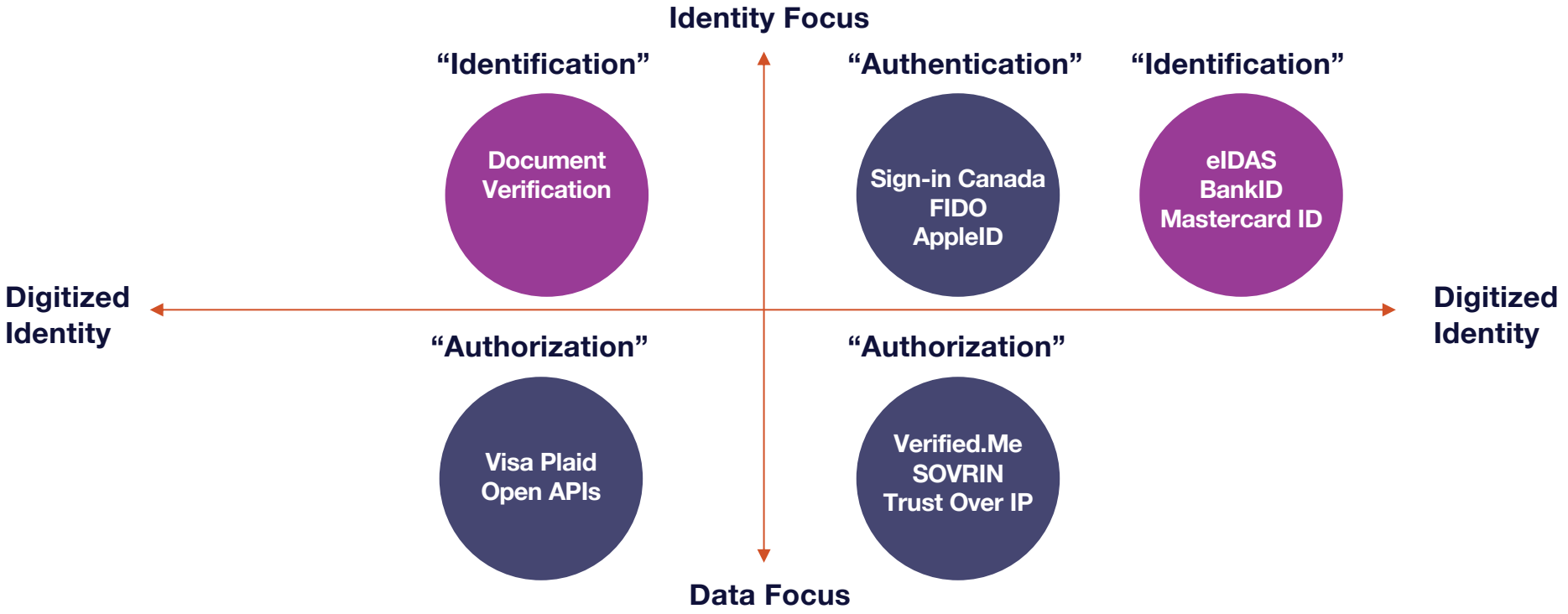
Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

Theme: Data Integrity

Ensuring the integrity of data is key to trusted digital identity. This has brought cryptography to the fore, especially in the development of Verifiable Credential standards.

What does digital identity look like today?



Theme: Identity vs Identification

Growing use of mobile document verification solutions for digital onboarding. By themselves they do not enable re-usable or portable digital identities.

Theme: Identity vs Data

Much focus on sharing of personal data. This includes proving identity or entitlement through the sharing of attributes. It also includes the broader sharing of personal and transactional data through open APIs. This blurring of the lines creates complex governance challenges.

Big tech companies that have amassed huge data are also increasingly dabbling with identity.

Theme: Data Integrity

Ensuring the integrity of data is key to trusted digital identity. This has brought cryptography to the fore, especially in the development of Verifiable Credential standards.

Theme: Governance

Decentralized identity standards enable the rails. Trust frameworks are needed to set the rules.

On the internet, nobody knows you're a dog

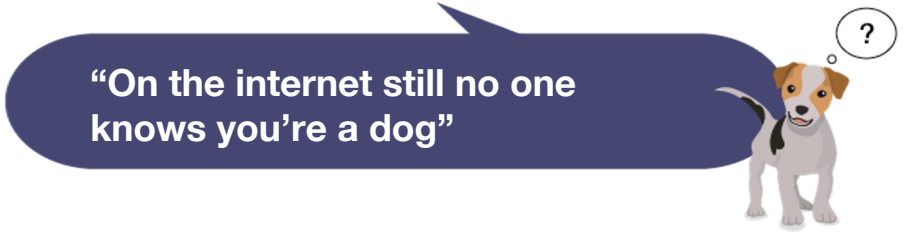
DIACC

Possible future scenarios

Possible future scenarios

Platform Identity

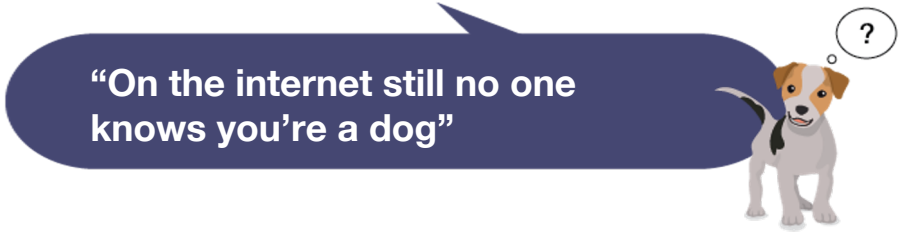
Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.



Possible future scenarios

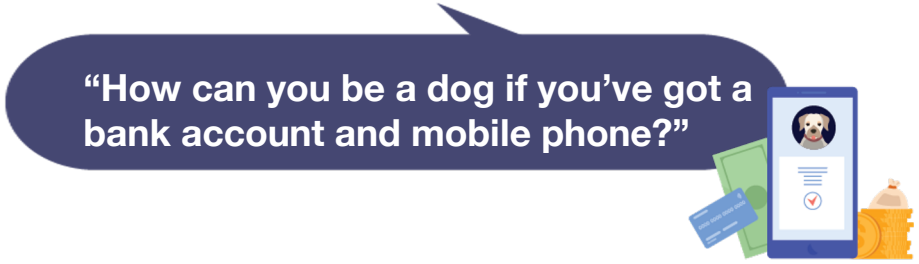
Platform Identity

Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.



Operator Networks

To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but it helps for services where identity matters the most.



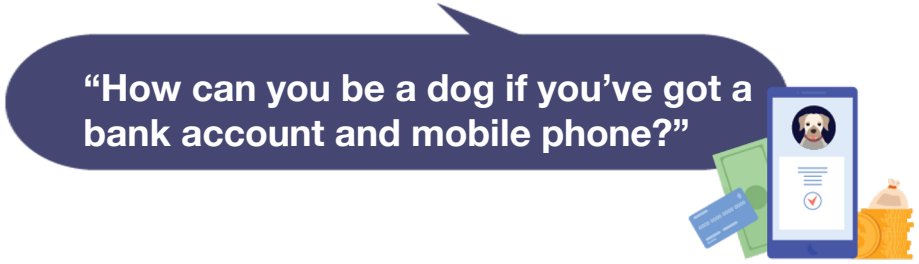
Possible future scenarios

Platform Identity

Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.

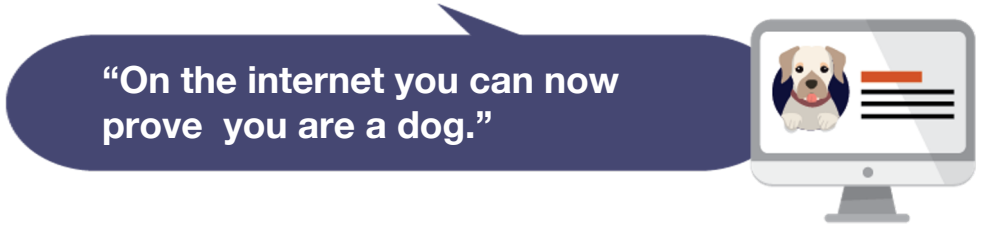
Operator Networks

To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but it helps for services where identity matters the most.



Self-Sovereign Identity

Users and businesses realize a need to fundamentally change personal data management. For businesses, personal data is a liability due to data protection risks. Users see the value of being able to hold data and take it where they need it. For this to work, data presented by users needs to be reliable and trustworthy. Some have started to use cryptographic wallets to collect and share signed data. Users need to look after their data, much like they look after their money.

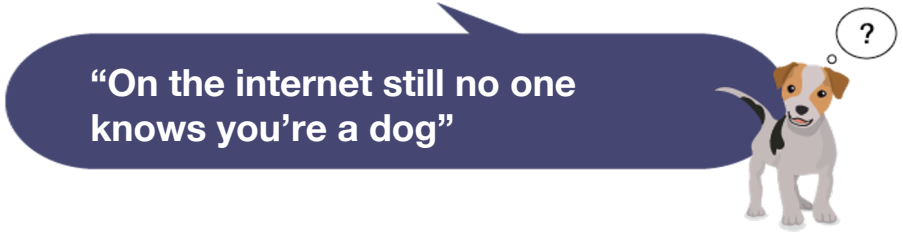


DIACC

Possible future scenarios

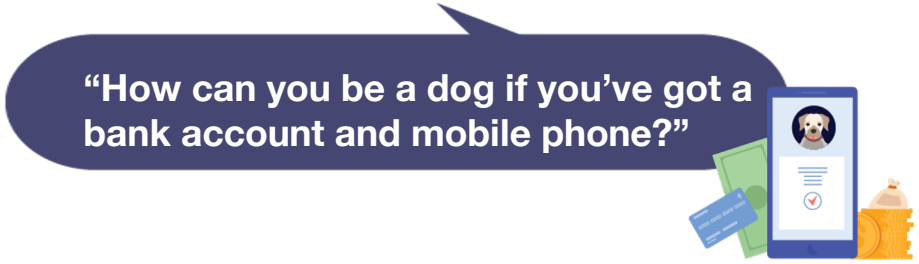
Platform Identity

Internet giants tried to adapt business models away from advertising revenues but consumers are not willing to pay. The net effect is that while additional regulatory controls are being placed around them, the system is still fundamentally the same. So end-users have limited visibility on what information is held about them or how it is used.



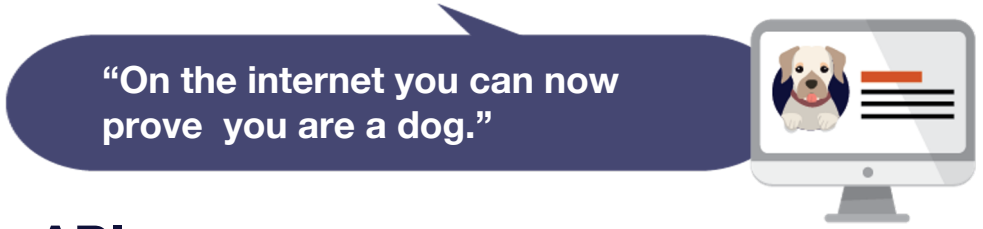
Operator Networks

To sign up and use secure digital services, users need to provide reliable information about their identity. Users trust regulated organizations to provide services like banking and protected internet access. It’s natural to look to the same organizations to help with digital identity. Secure identity exchange networks help responsible organizations to share user information, with the user’s consent. It may not work everywhere but it helps for services where identity matters the most.



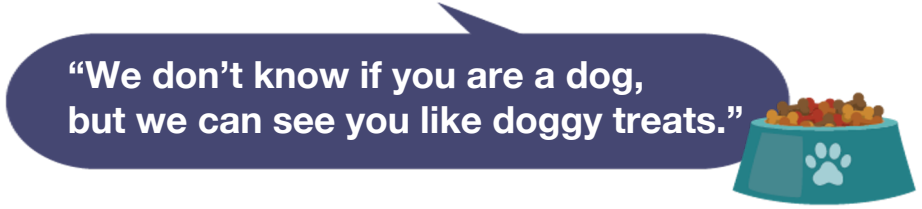
Self-Sovereign Identity

Users and businesses realize a need to fundamentally change personal data management. For businesses, personal data is a liability due to data protection risks. Users see the value of being able to hold data and take it where they need it. For this to work, data presented by users needs to be reliable and trustworthy. Some have started to use cryptographic wallets to collect and share signed data. Users need to look after their data, much like they look after their money.



Open APIs

Organizations across the economy have been forced to open APIs allowing services to access user data (with the user’s consent) from other places. Users link together different services as the need arises. It is down to the individual service to piece together all the data it collects into something meaningful for the particular user. Most individual users don’t remember all the connections and links they have set up.



DIACC

What are the key challenges that need attention?

DIACC's role in scenarios

How well would scenarios align with the values of DIACC members?

Requirement	Platform	Operator Networks	Self-Sovereign	Open APIs
Participation	L	H	M	M
Transparency	L	M	H	L
Accountability	L	H	M	L
Confidentiality	L	H	H	H
Integrity	L	H	H	M
Availability	M	H	H	M

What influence does the DIACC currently have?

Platform	Operator Networks	Self-Sovereign	Open APIs
None	Good	Good	Limited

The above high-level evaluation of each of the scenarios is based on the governance and operational requirements as described in DIACC's whitepaper "Making Sense of Identity Networks", which reflects DIACC member values and expectations for identity networks. More detail behind the intent of each requirement is included in the appendix of this document.

This evaluation demonstrates that the self-sovereign and operator network scenarios are best aligned with DIACC member values, with the open APIs scenario providing challenges particularly in governance, and the platform scenario being the least aligned.

What key challenges are common across future scenarios?

What key challenges are common across future scenarios?

Creating Market Conditions

Standards

The source of authority for digital identity standards across the economy is unclear due to parallel working body efforts across Canada.

Regulatory

Government has an important role to play in digital identity. The provinces and territories are primary sources of foundational identities. Regulation needs to allow digital identity solutions, including the controlled opening up of data.

What key challenges are common across future scenarios?

Creating Market Conditions

Standards

The source of authority for digital identity standards across the economy is unclear due to parallel working body efforts across Canada.

Regulatory

Government has an important role to play in digital identity. The provinces and territories are primary sources of foundational identities. Regulation needs to allow digital identity solutions, including the controlled opening up of data.

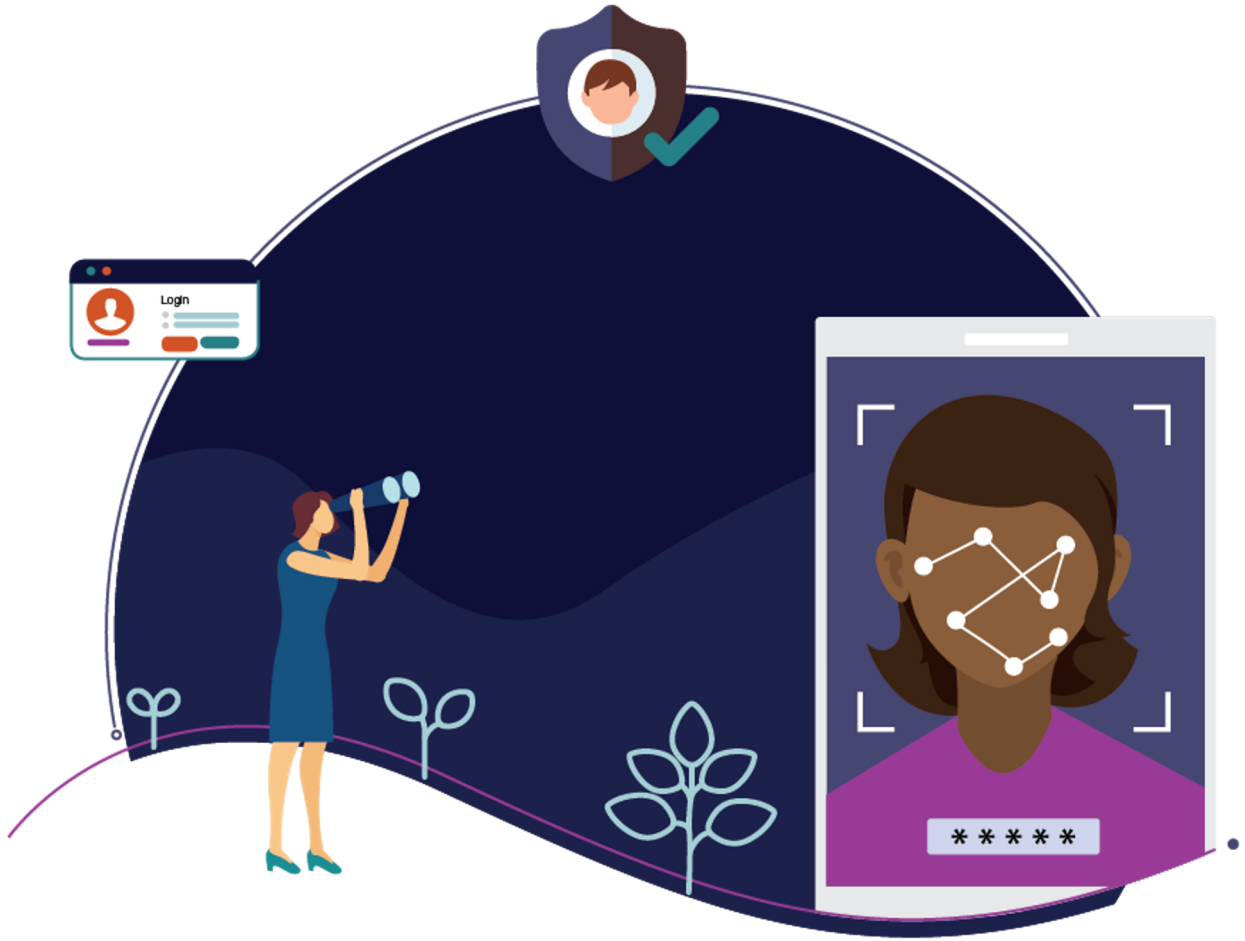
Promoting Market Growth

Sustainability

While each scenario provides a varying perspective, commercial sustainability and viability are either unclear, underdeveloped, or unproven. Considerations for liability should also be included in this category of challenges as the responsibility around personal data exchanged needs to be carefully examined.

Inclusion

Ensuring that a critical mass of providers and users adopt digital identity products is significant across all scenarios, while also ensuring those that are typically excluded can get access to services or can be provided with better experiences than those that exist today.



How do we ensure that identity will respect citizens and consumers?

Canadians' Perspectives on Digital Identity

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians' Perspectives on Digital Identity

70%

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Canadians' Perspectives on Digital Identity

70%

feel that a collaboration between the government and the private sector is the **best approach to creating a pan-Canadian digital ID framework**.

DIACC

Source: https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/

Bill 64: Overhaul of Quebec's Privacy Law Regime

- Significant sanctions may be imposed by Commission d'accès à l'information ("**CAI**") up to $10 million or 2% of worldwide turnover, whichever is greater, and penal sanctions up to $25 million or 4% of worldwide turnover.
- Possibility for a company to be sued for damages.
- Requirement to appoint a Chief Privacy Officer and establish governance policies and practices.
- New obligations when a data breach incident occurs.
- New rights for individuals for data portability, right to be forgotten and right to object to automated processing of their personal information.
- Creation of exception allowing disclosure of personal information in the course of a business transaction without prior consent of individuals concerned.
- Remove for businesses the possibility of communicating, without the consent of persons concerned, nominative lists and new rules governing the use of personal information for commercial or philanthropic prospecting purposes.
- Obligation for companies to ensure pre-established settings for technology products and services ensuring highest levels of confidentiality by default. (privacy by design)

DIACC

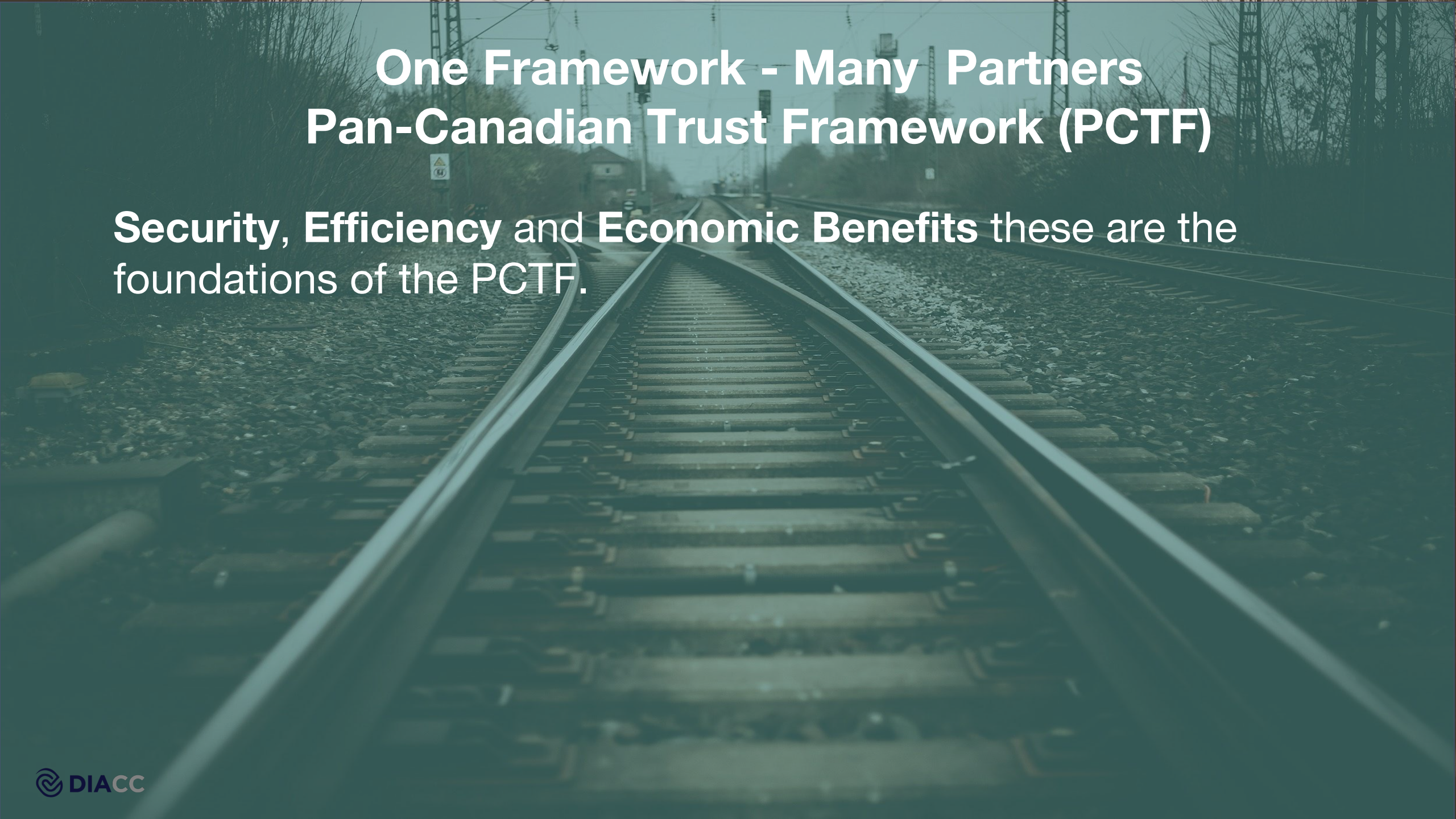
Source: https://www.mccarthy.ca/en/insights/blogs/techlex/bill-64-overhaul-quebecs-privacy-law-regime-implications-business

One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

DIACC

One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.



DIACC

One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.

Led by the DIACC with **multi-sectoral pan-Canadian and international input**, the PCTF is connecting and enabling Canada's digital economy from coast-to-coast-to-coast.

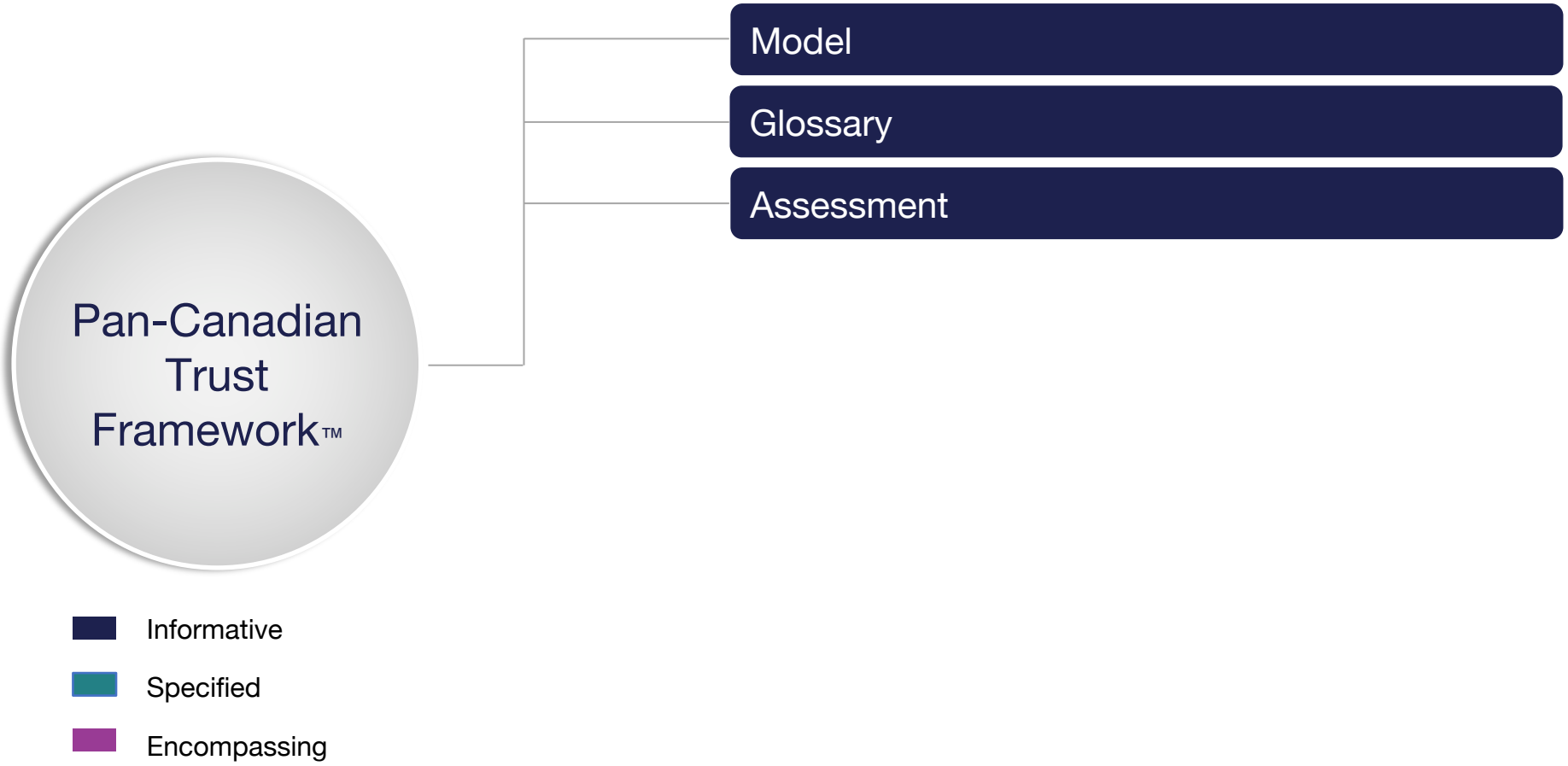
One Framework - Many Partners
Pan-Canadian Trust Framework (PCTF)

Security, **Efficiency** and **Economic Benefits** these are the foundations of the PCTF.

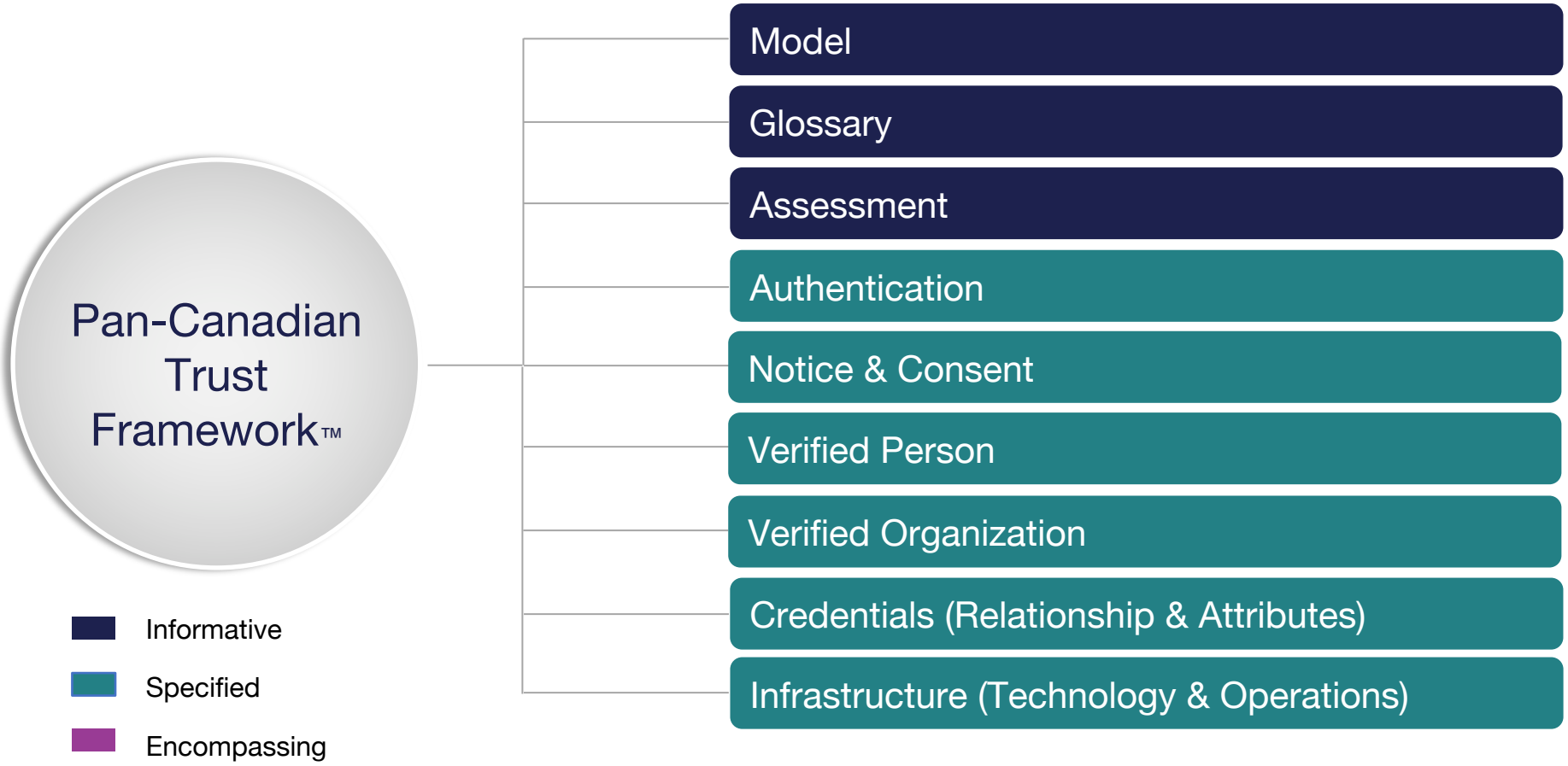
Led by the DIACC with **multi-sectoral pan-Canadian and international input**, the PCTF is connecting and enabling Canada's digital economy from coast-to-coast-to-coast.

Developed to secure **cross-sector identity interoperability** with a focus on industry standards and practices. PCTF is available @ **DIACC.ca**

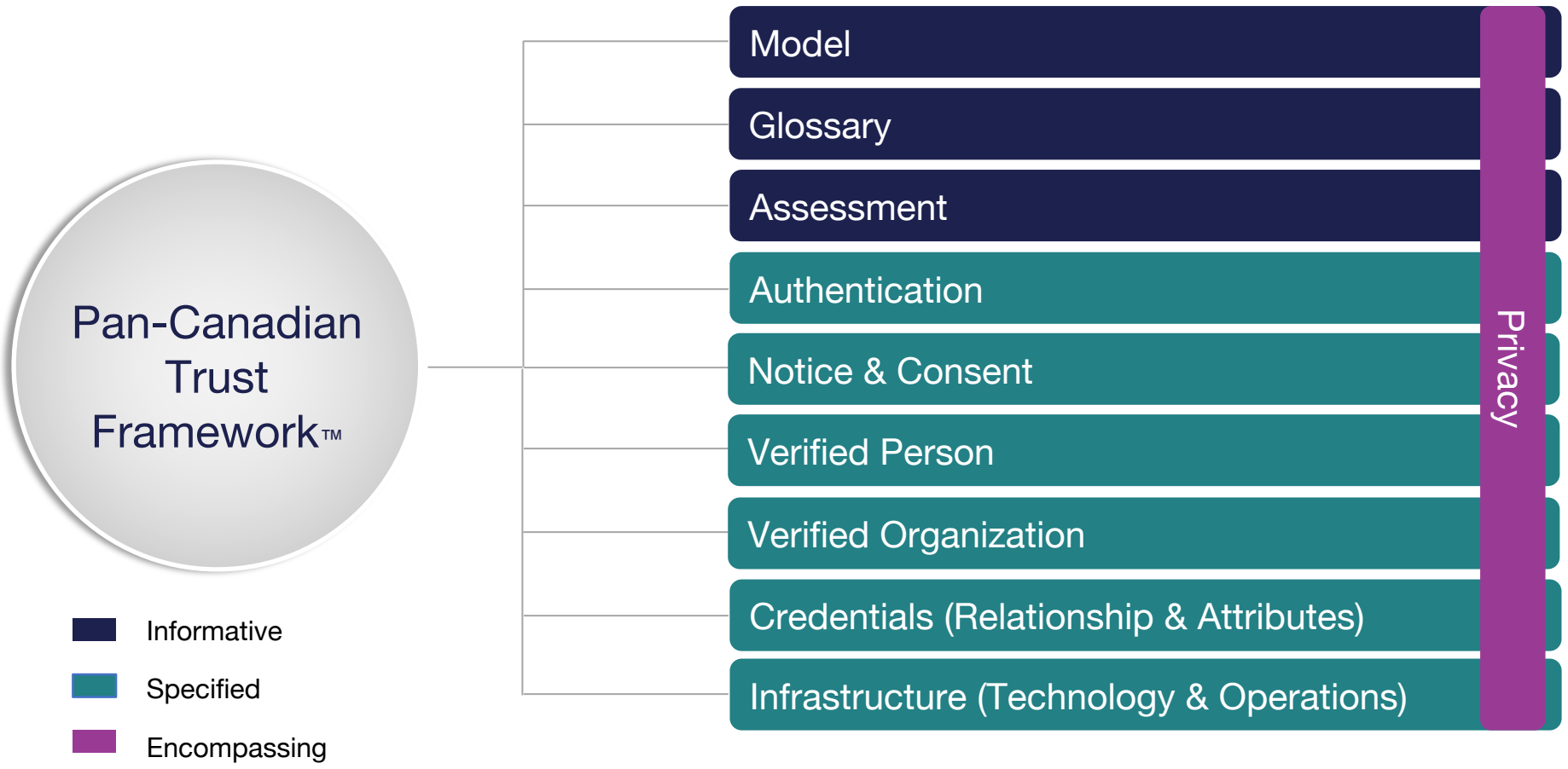
A Pan-Canadian Trust Framework for Digital Services



A Pan-Canadian Trust Framework for Digital Services



A Pan-Canadian Trust Framework for Digital Services



A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework™**

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

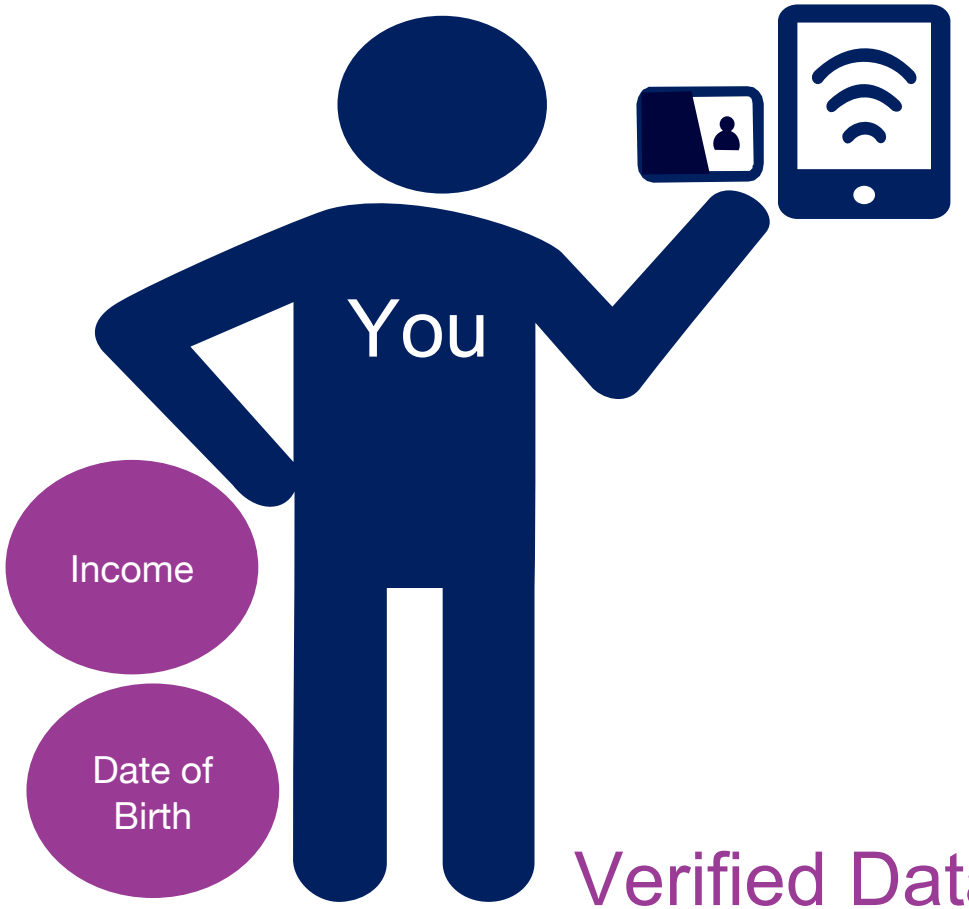
DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More



Verified Data

Data Requesters

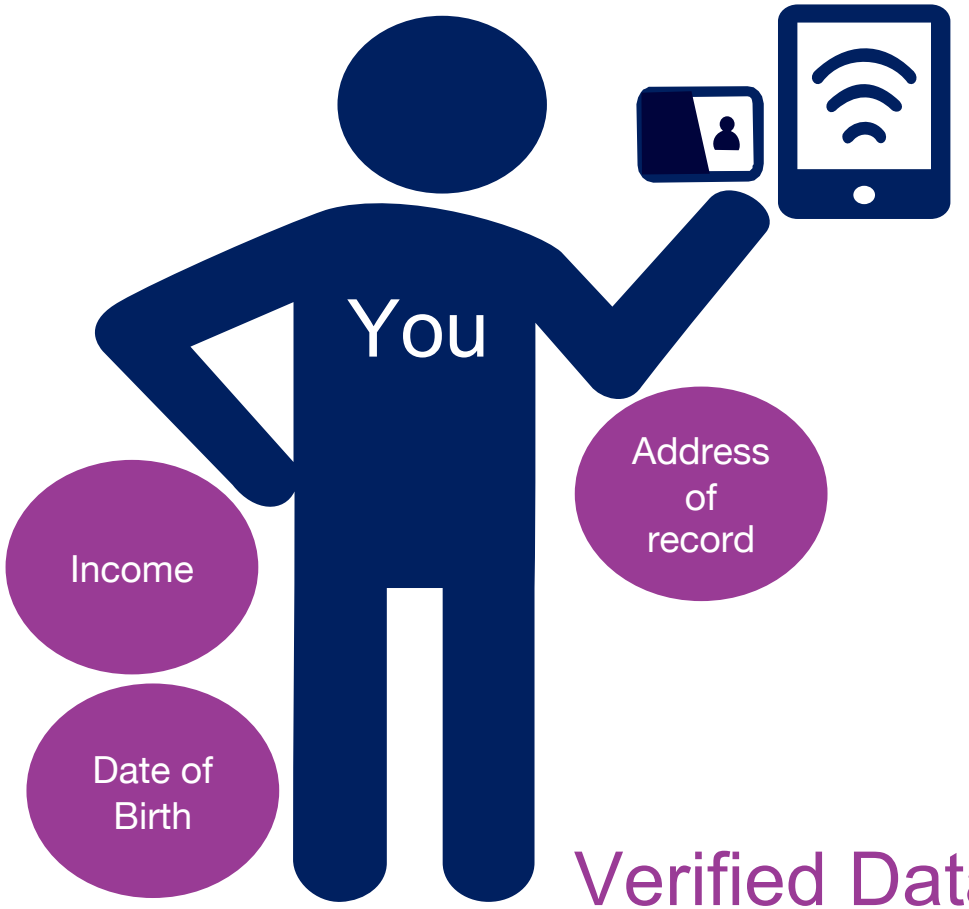
- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More



Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

DIACC

A Framework to Unlock Identity Networks Utility

Consent, privacy, ethical use of identity information
with the **Pan-Canadian Trust Framework**™

Data Verifiers

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

Data Requesters

- Governments
- Universities
- Banks
- Telco Providers
- Credit Agencies
- More

DIACC

How would digital identity be used?

Digital Identity Use Cases: Government Services

Public Service/Policymakers can:

- Increase efficiencies in a highly regulated system by replacing the printing and resubmitting of forms from separate government departments with a digital ID-powered system
- Improve integrity of communication (phone calls, emails), as digital ID dramatically increases the certainty that the government is interacting with the correct person.
- Provide a more client-centric approach to serving the public by putting Canadians at the centre of digital ID solutions so that the government can change how interactions with Canadians are designed.
- Have less frequent data entry errors and higher data quality. Digital ID consent mechanisms that enable the sharing of data for research would lead to better policy direction and outcomes.
- Be innovative, by creating new ways of providing services to Canadian citizens and businesses and transform how government policies work.

Businesses can:

- Overcome cumbersome manual processes (such as business registration, licensing, permitting and inspections) for more efficient interactions with local, provincial and federal government departments.

Citizens can:

- Access services they need quicker and more efficiently by providing consent to share their data across departments. This can decrease in-person appointments and paper application processes and increase accessibility for those living in rural and remote communities by mitigating needs for commutes.
- Navigate the government administrative processes with more confidence and ease. With a unique digital ID, citizens can “log into” government services, similar to how they log into a bank account and access their services all in one place.

Digital Identity Use Cases: Health Care

Patients can:

- Seamlessly and securely access health documents in one place
- View test results, giving control over personal records and increased ability to advocate
- Integrated and unified health care records that enable more efficient and error-free point of care
- Access to health services any time, anywhere, securely authenticating identity to connect to health professionals on any device

Practitioners & Organizations (clinics, hospitals, paramed, medical research) can:

- Enhance operational efficiencies, including those related to records management and reporting, and care management.
- Reduce chances of prescription fraud with enhanced digital association between identity, prescription, and pharmacy fulfilment. Prescriptions for drugs like opioids and other controlled substances can have increased validation and verification requirements in order to fill the prescription.
- Access quality information about patients. Gated and segmented health records can be shared digitally between health professionals with a patient's permission for a robust medical history.
- Increase time for doctors and clinical researchers by decreasing the time needed to log in and out of applications to verify practitioner identity

Policy-makers (Government) can:

- Develop better informed policy decisions with the access of higher quality data, which can improve accuracy of future health care research and ensure actions taken are truly patient-first.

Digital Identity Use Cases: Commerce

Consumers can:

- Easily facilitate transactions by connecting their payment services provider to retailers.
- Minimize their risk of identity theft and privacy breaches with data minimization established - consumers provide their information on an as-needed basis, protecting their privacy and preserving anonymity.

Businesses can:

- Improve processes for remotely conducting transactions from distant geographic locations.
- Benefit those working in the ‘gig economy’ (i.e. freelancers and Uber drivers) with remote authentication across digital channels. With one click, platforms like Uber can verify these workers, and they could be trusted by both the platforms and customers.

E-commerce Businesses can:

- Reduce their risk for customer fraud or breaches by accessing only need-to-know details.
- Have the ability to perform Know Your Customer (KYC) checks to satisfy regulator requirements is key for providers. KYC procedures are also a legal requirement in order to comply with Anti-Money Laundering (AML) laws. KYC refers to the steps taken to establish customer identity, understand the nature of their activities and assess AML risks. Having a digital ID system in place would enable this.
- Conduct peer-to-peer sales more securely with verified identity, such as on eBay or AirBnB.
- Minimize administrative customer issues, which can impact their productivity and bottom line, such as minimizing the number of people calling in for password resets and errors in delivery logistics.
- Increase their probability of customer loyalty and retention by providing customers with a more structured and secure sales process.

Retailers (in-person) can:

- Accurately and securely verify the shopper’s age when selling restricted goods and content.
- Reduce commercial transaction times and/or costs with automation (i.e. faster interactions at the check out), resulting in increased efficiency.

Digital Identity Use Cases: Finance

Financial Institutions (FIs) can:

- Streamline their business processes, from customer registration and transaction monitoring, to credit risk assessment, ultimately offering an improved service delivery. A more streamlined authentication process can also result in increased sales of goods and services, helping with customer retention.
- Increase their cost savings through reduced fraudulent activity, as digital ID can make it easier to verify and trust FI's customer bases.

Clients and consumers can:

- Place greater trust in their FIs knowing that a secure digital ID system has been adopted.
- Have more control over their data and identity, as data that is shared will be on a need-to-know basis.
- Gain greater accessibility to financial services that are currently hindered by lack of documentation, distance to financial institutions, and cost of financial services for many people worldwide.
- Save on transaction costs, with fewer or no service fees, as well as an elimination of the need for physical proof and exchange of paperwork in financial transactions.
- Access their services with speed and ease as a streamlined and efficient process makes for a faster turnaround time for verification and authentication.

Digital Identity

Digital Identity
done right requires
public and private sector
collaboration

The Digital ID & Authentication Council of Canada

Leading Canada's **full and beneficial global digital economy participation** by delivering a **digital identity and authentication interoperability framework.**

The DIACC is a **Non-profit coalition** of **public and private sector members** created as a result of federal government's Electronic Payments System Task Force.

DIACC Board

Treasury Board of Canada Secretariat

British Columbia

Ontario

New Nouveau Brunswick

BMO

CIBC

Canada Post Postes Canada

Desjardins

ForgeRock

Interac

Manulife

SecureKey

TD

TELUS

Sustaining Members

cdic sadc

Canada Deposit Insurance Corporation

Société d'assurance-dépôts du Canada

RBC

Saskatchewan

Sustaining Members

mastercard

EQUIFAX

Vancity

Sustaining Members



Adopter Members: Canadian Council of Motor Transport Administrators, Niagara Health

Join the Conversation!

Adopt the Pan-Canadian Trust Framework to secure the foundation of digital identity that will secure Canada's digital transformation.

Contact us to join the conversation info@diacc.ca

diacc.ca @mydiacc /company/mydiacc /mydiacc

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

LES IMPACTS JURIDIQUES DES INCIDENTS DE CYBERSÉCURITÉ

JOCELYN AUGER
Associé, BCF Avocats d'affaires

BCF AVOCATS D'AFFAIRES

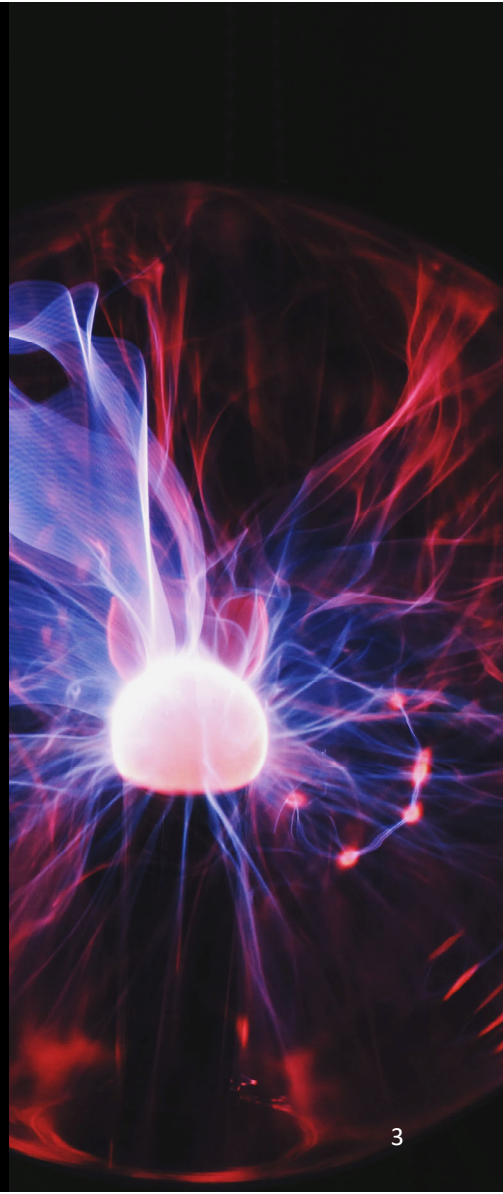
CONFÉRENCE CYBER SÉCURITÉ 2020

ÉDITION VIRTUELLE

ORDRE DU JOUR

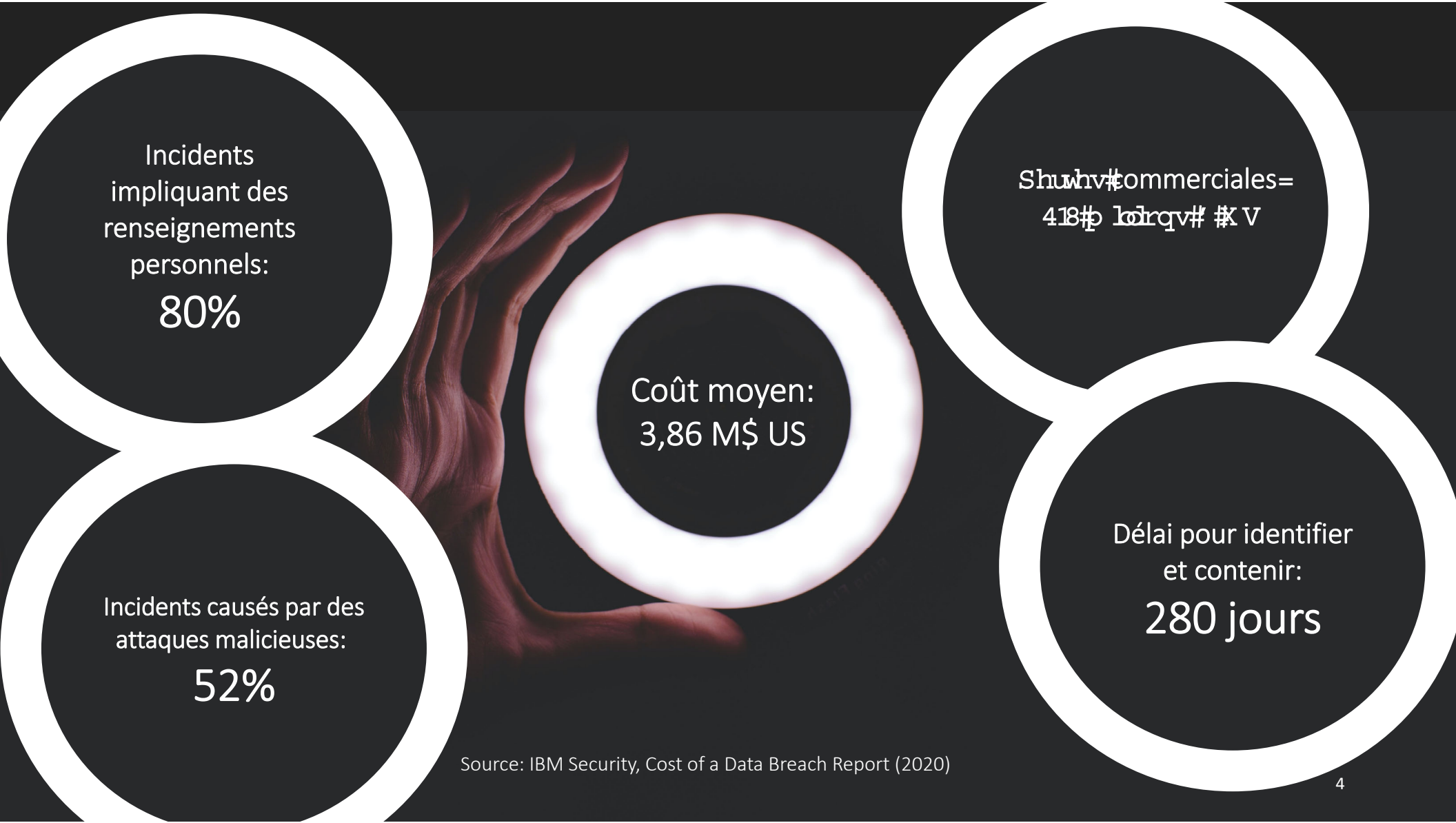
- Contexte: statistiques intéressantes
- Sources d'obligations juridiques
- Impacts et conséquences juridiques
  - Court terme: 0 – 3 mois
  - Moyen terme: 3 mois – 3 ans
  - Long terme: > 3 ans
- Atténuation des risques juridiques

Statistiques intéressantes



Incidents impliquant des renseignements personnels:
80%

Incidents causés par des attaques malicieuses:
52%



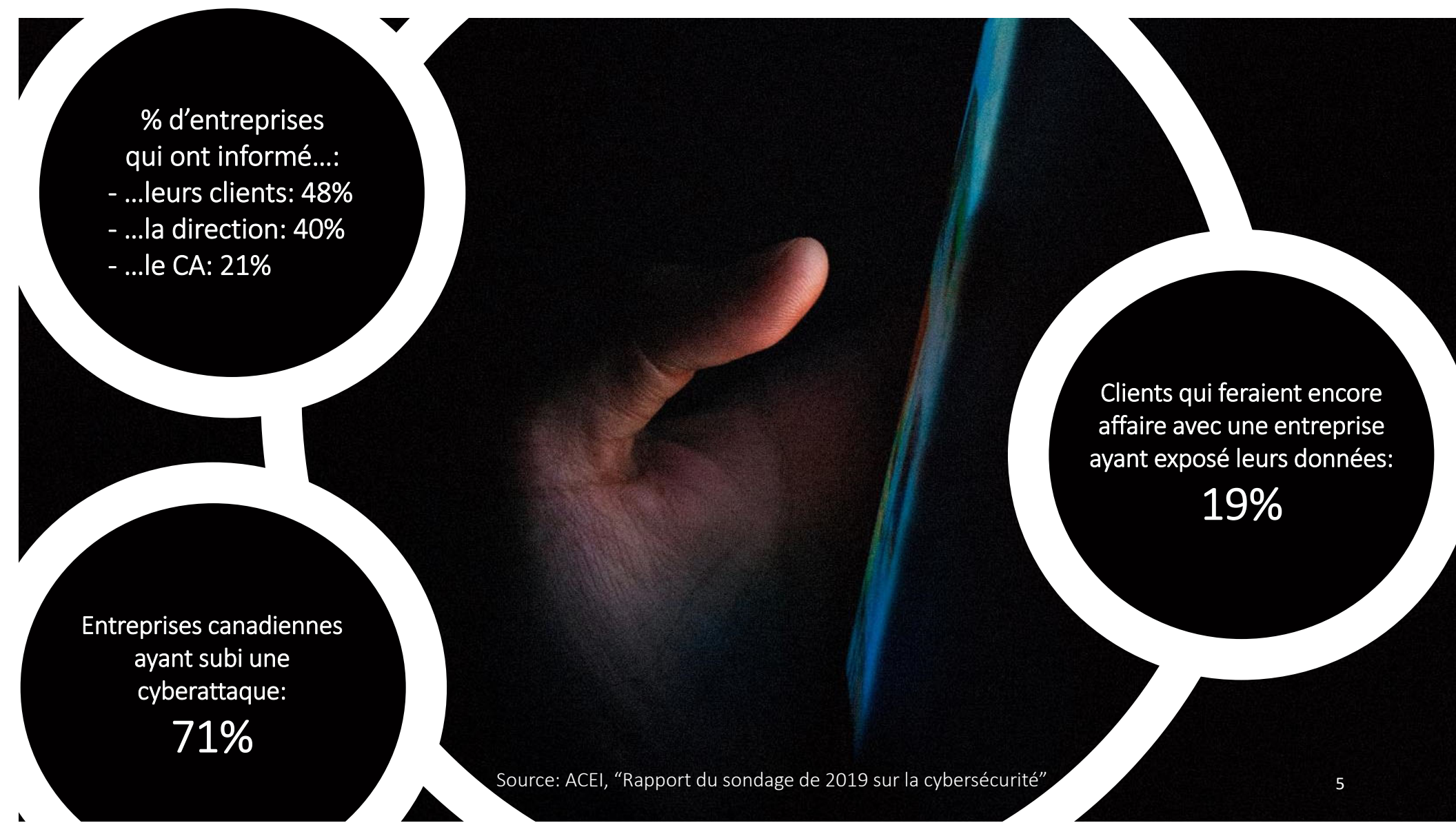
Coût moyen:
3,86 M$ US

Shuwv#commerciales=
418#p lodrqv# #XV

Délai pour identifier et contenir:
280 jours

Source: IBM Security, Cost of a Data Breach Report (2020)

% d'entreprises qui ont informé…:
- …leurs clients: 48%
- …la direction: 40%
- …le CA: 21%

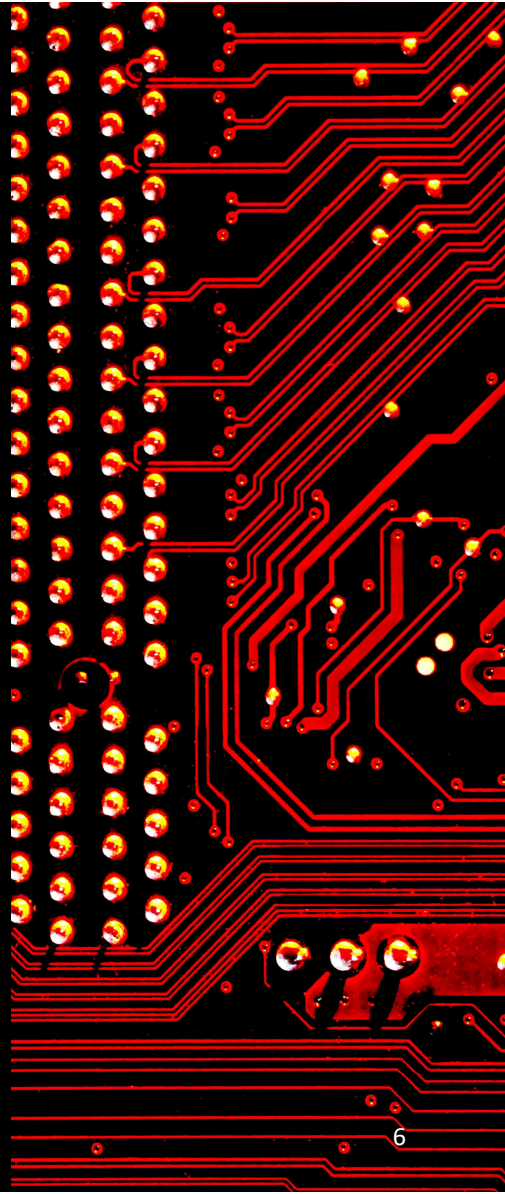


Clients qui feraient encore affaire avec une entreprise ayant exposé leurs données:
19%

Entreprises canadiennes ayant subi une cyberattaque:
71%

Source: ACEI, "Rapport du sondage de 2019 sur la cybersécurité"

Sources d’obligations juridiques



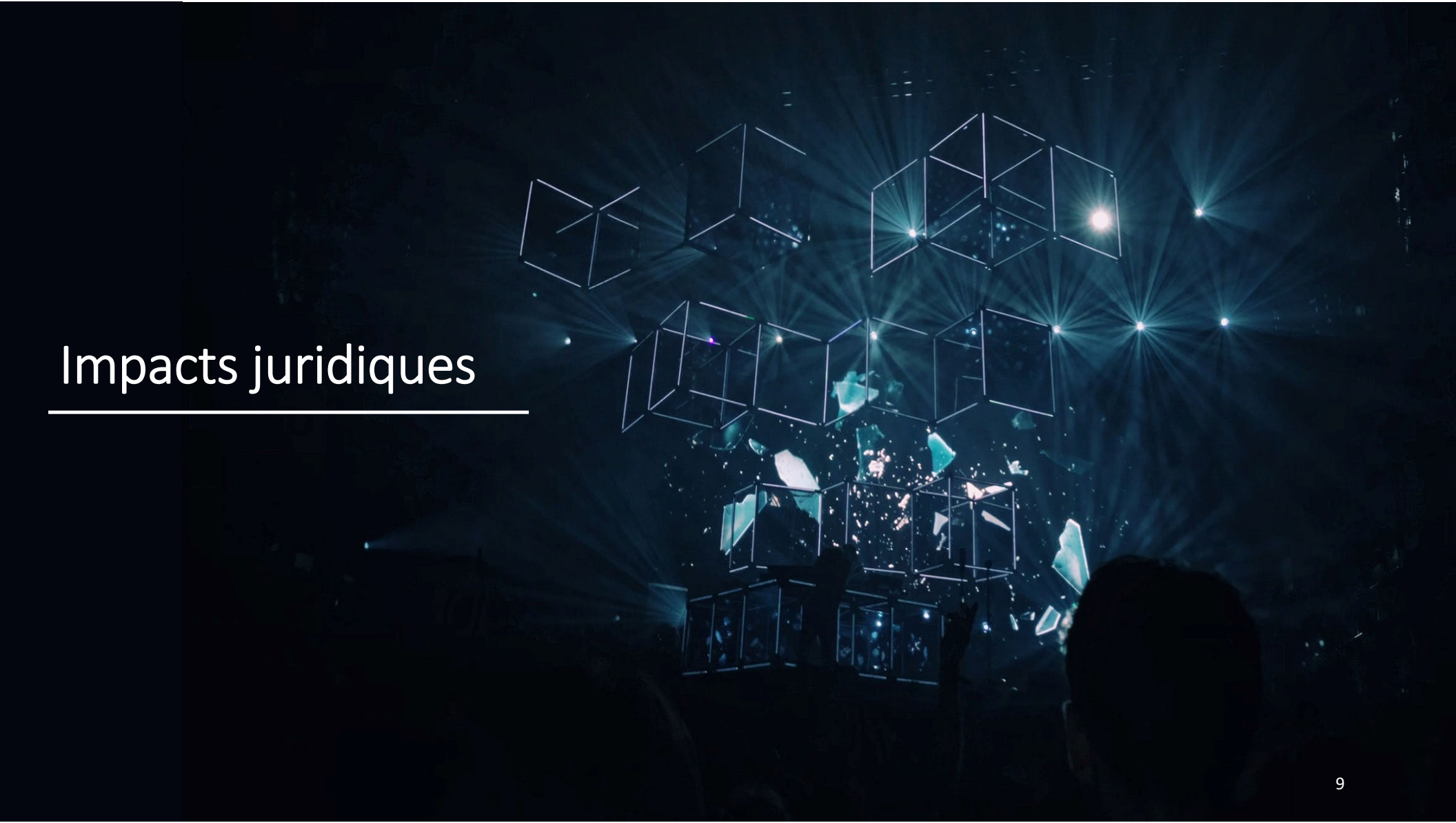
Sources d’obligations: Lois et règlements

- Lois sur la protection des **renseignements personnels** (LPRSP, LRPDE, RGPD)
- Lois et règlements dans les domaines de:
  - **Valeurs mobilières** (émetteurs assujettis, sociétés publiques)
  - **Télécommunication**
  - **Services financiers** (banques, assurance, placement)
  - **Services et soins de santé**

Sources d'obligations: Contrats

- Ententes et clauses de confidentialité
- Ententes de traitement de données (*Data Processing Agreements*) et équivalents
  - de plus en plus fréquentes depuis l'entrée en vigueur du RGPD
  - Obligatoires sous les nouvelles lois québécoise et fédérale
- Politiques de protection des renseignements personnels (*Privacy Policies*)

Impacts juridiques



Impacts juridiques à court terme: 0 – 3 mois

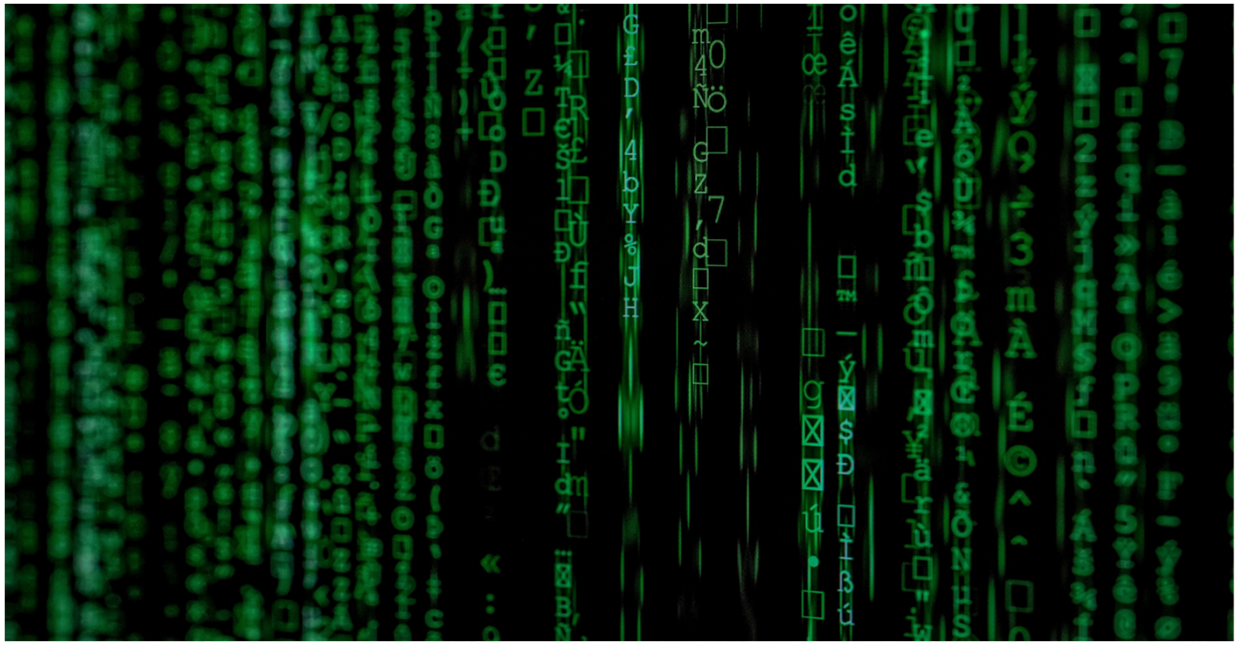
- Notification/divulgation de l’incident
- Enquêtes règlementaires
- Communications/Relations publiques:
  - Ce que vous direz (ou ne direz pas) pourra être retenu contre vous…
  - En fait, ce que l'on ne dit pas est souvent pire que ce que l'on dit

Impacts juridiques à moyen terme: 3 mois – 3 ans

- Recours contractuels:
  - Manquement à des engagements contractuels
- Recours règlementaires/pénaux
  - Nouvelles lois donnent des pouvoirs d'enquête élargis;
  - Amendes considérables: jusqu'à 25M$ ou 4-5% du chiffre d'affaires mondial
    - 19 amendes en 2020, totalisant 135M€;
    - Variant entre 100k€ et 50M€ (Google France).

Impacts juridiques à moyen terme: 3 mois – 3 ans (suite)

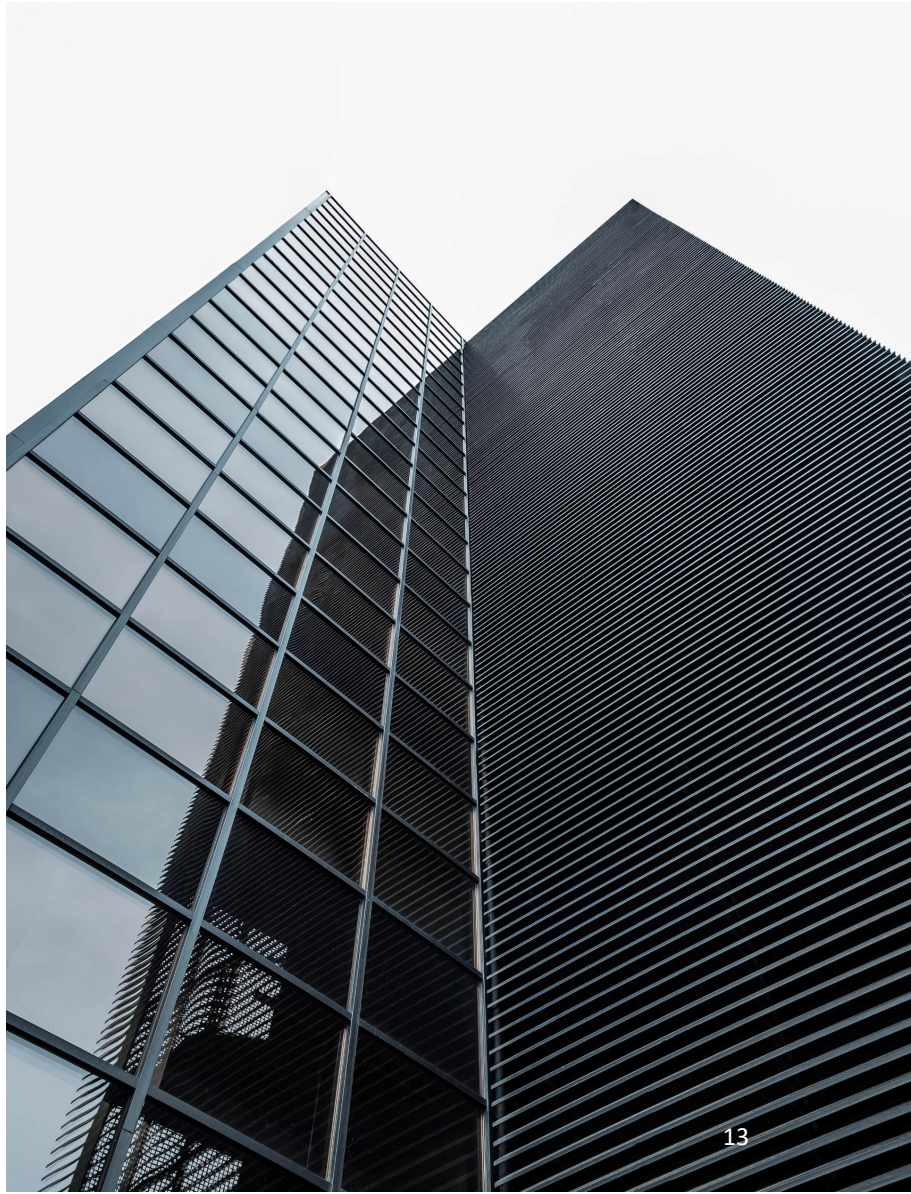
- Le plus coûteux: Actions collectives



Impacts juridiques à long terme: >3 ans

Fusions et acquisitions

- Peut influencer le résultat d'une transaction d'acquisition
  - Ex. Marriot International et Starwood
  - Vérification diligente accrue
  - Représentations et garanties; indemnisations spécifiques



Atténuation des risques juridiques

Atténuation des risques juridiques

- Gouvernance:
  - Nommer un responsable de la protection des données (DPO)
  - Adopter des politiques écrites, plan de réponse aux incidents
    - Auditer et tester l'application des politiques
- Formation des employés
- Implanter des contrôle d'accès
- Mesure de surveillance (attention à l'abus!)
- Assurance cyber-risques

Jocelyn Auger

Associé / Avocat
514 397 2643
jocelyn.auger@bcf.ca

1100 Boulevard René-Lévesque Ouest
25 étage,
Montréal, QC
H3B 5C9

Remerciements à Salvatore Tedone pour l'assistance dans la preparation de cette présentation

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

LES ASSOCIATIONS EN CYBERSÉCURITÉ : LEUR RÔLE ET LEUR APPORT ESSENTIEL POUR LES ACTEURS ÉCONOMIQUES QUÉBÉCOIS

CONFÉRENCE CYBER SÉCURITÉ 2020

ÉDITION VIRTUELLE

ASIMM

ASIQ ASSOCIATION DE LA SÉCURITÉ DE L'INFORMATION DU QUÉBEC

ISACA Fiabilisez, optimisez et rentabilisez les systèmes d'information Section de Montréal

cyber eco

IN·SEC·M INNOVATION · SÉCURITÉ · MARCHÉ

DOMINIQUE DERRIER
Association de Sécurité de l'Information du Montréal-Métropolitain **(ASIMM)**

ELHADJI NIANG
Association de la sécurité de l'information du Québec **(ASIQ)**

MARCEL LABELLE
Cyber eco

NICOLAS DUGUAY
In-Sec-M

YAN HUARD
Information Systems Audit and Control Association **(ISACA)**

Généralistes
Rendre accessible

Les Normes
Certifications

ASIMM

ASIQ

ISACA

CYBER ECO

INSEC-M

Développement de projets
Relations d’affaires

CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM

01

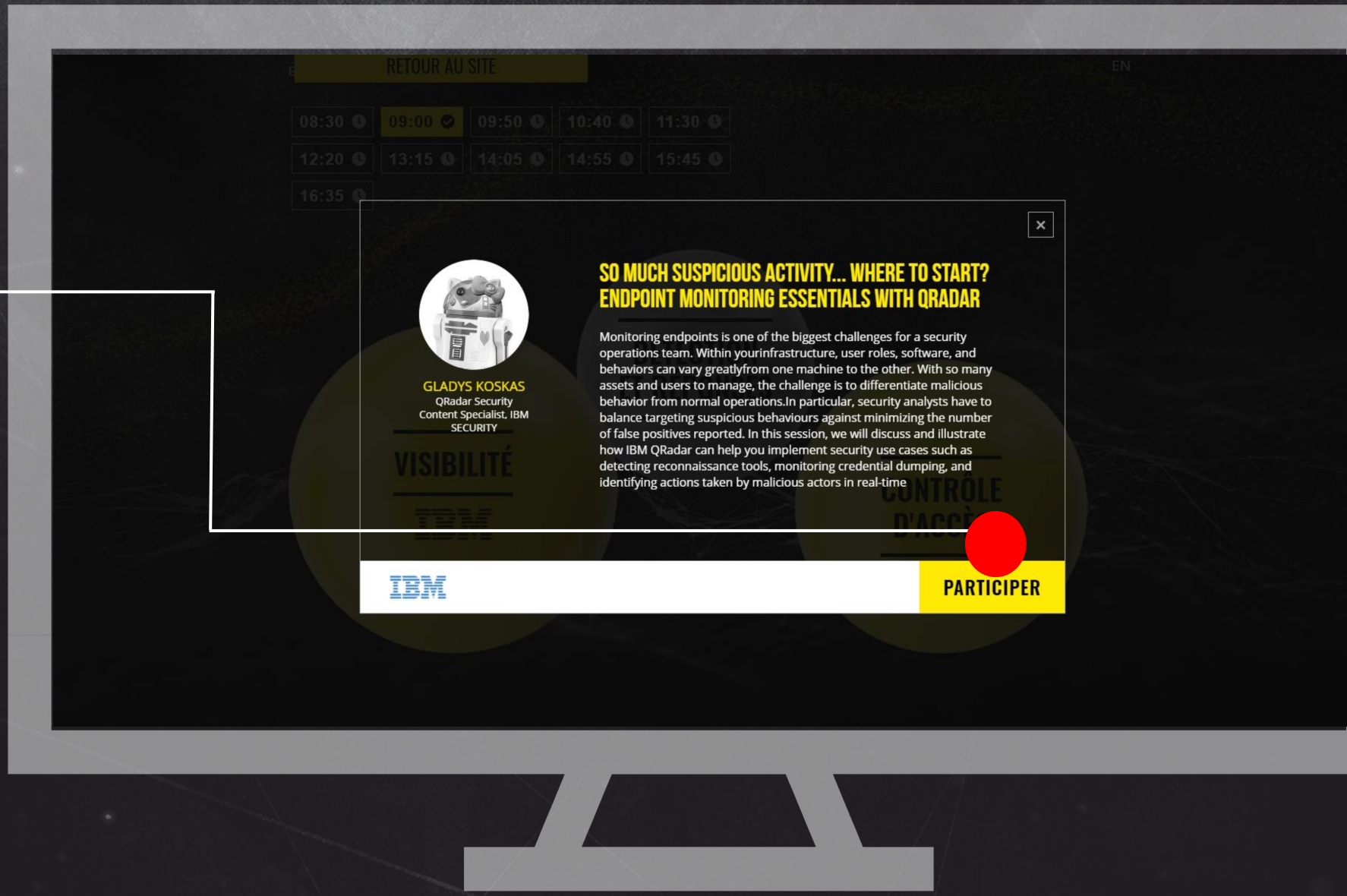
Sélectionnez une plage horaire

02

Cliquez sur la bulle thématique de votre choix

03

Cliquez sur **PARTICIPER** pour débuter le visionnement



CONFÉRENCE CYBER SÉCURITÉ 2020

Présenté par :

NOVIPRO

En collaboration avec :

IBM