Télétravail et outils de collaboration

Comment les pirates vous ciblent aujourd'hui ?

Patrick Mathieu, Hackfest.ca

Octobre 2020

ISACA Section de Québec

Qui suis-je?

Bonjour!

Patrick Mathieu

- Hacker depuis 20+ ans
- Senior Offensive Security Manager @ LogMeIn.com
- Co-fondateur de Hackfest.ca depuis 12 ans
- R&D / Hobby / Community / Medias / OSINT

Twitter: @pathetiq
LinkedIn: https://www.linkedin.com/in/patrickrmathieu/
Email: patrick@hackfest.ca

Hackfest: https://hackfest.ca
Podcast: https://securite.fm


Shameless plugs

Podcast international sur la sécurité et le hacking.
Nouvelles et opinions du Québec et de l'Europe!

https://securite.fm

InfosecJobs

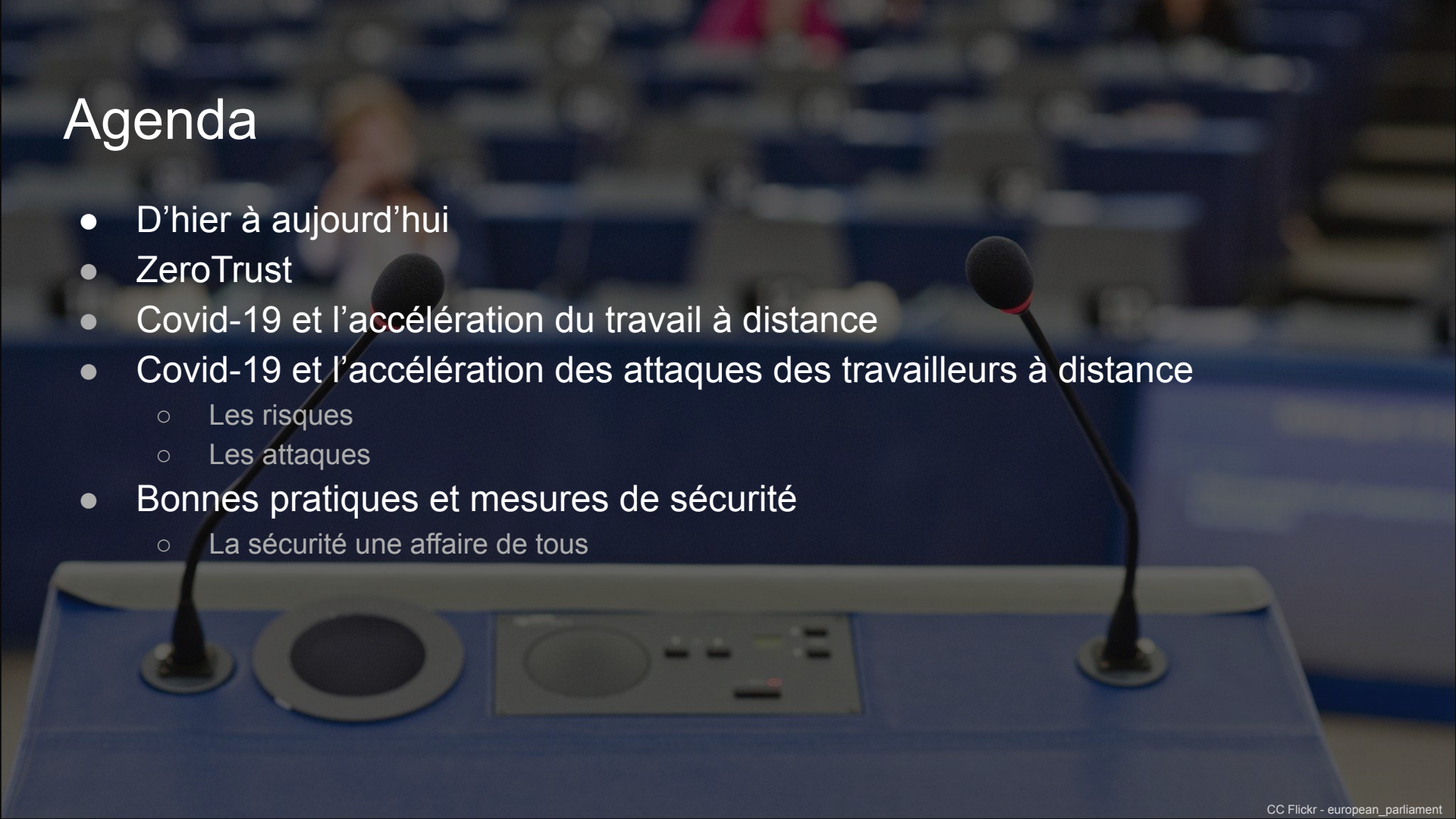
https://infosecjobs.ca


HACKFEST.ca
GET
INVOLVED
info@hackfest.ca

https://discord.gg/39fRfa6

Agenda

- D’hier à aujourd’hui
- ZeroTrust
- Covid-19 et l’accélération du travail à distance
- Covid-19 et l’accélération des attaques des travailleurs à distance
  - Les risques
  - Les attaques
- Bonnes pratiques et mesures de sécurité
  - La sécurité une affaire de tous



D’hier à aujourd’hui

Le passé - Le périmètre

Le passé c’était aussi la phrase:

“Oui, mais on a un Firewall?”

Ou encore on en a mis 3, donc notre application est sécuritaire!

Un firewall, ça reste une porte ouverte, surtout en Web!

Mauvaise sécurité Interne


Les criminels ne
suivent pas vos règles

ZeroTrust

The BeyondCorp Story

When a highly sophisticated APT attack named Operation Aurora occurred in 2009, Google began an internal initiative to reimagine their security architecture with regards to how employees and devices access internal applications.

Google

présentation public

https://static.googleusercontent.com/media/research.google.com/fr//pubs/archive/43231.pdf

SECURITY

BeyondCorp: A New Approach to Enterprise Security

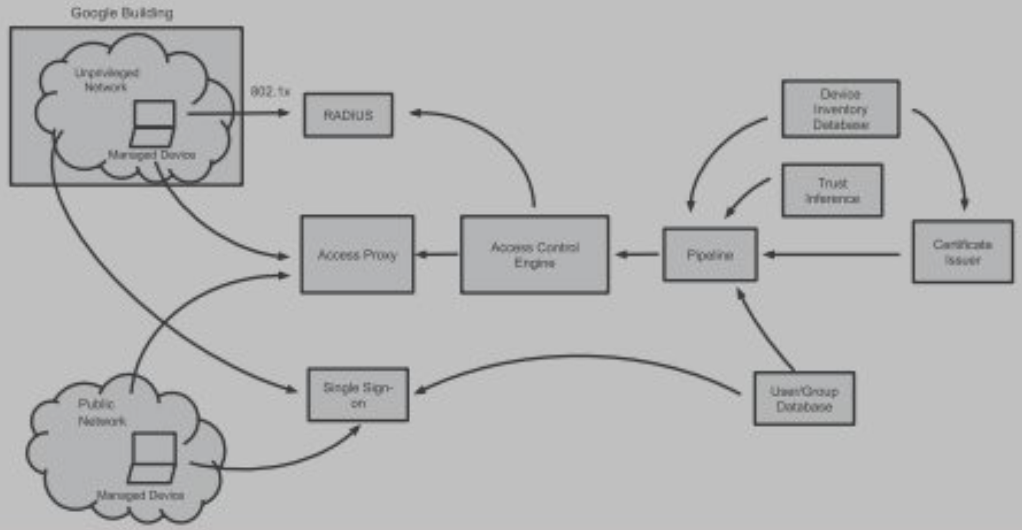
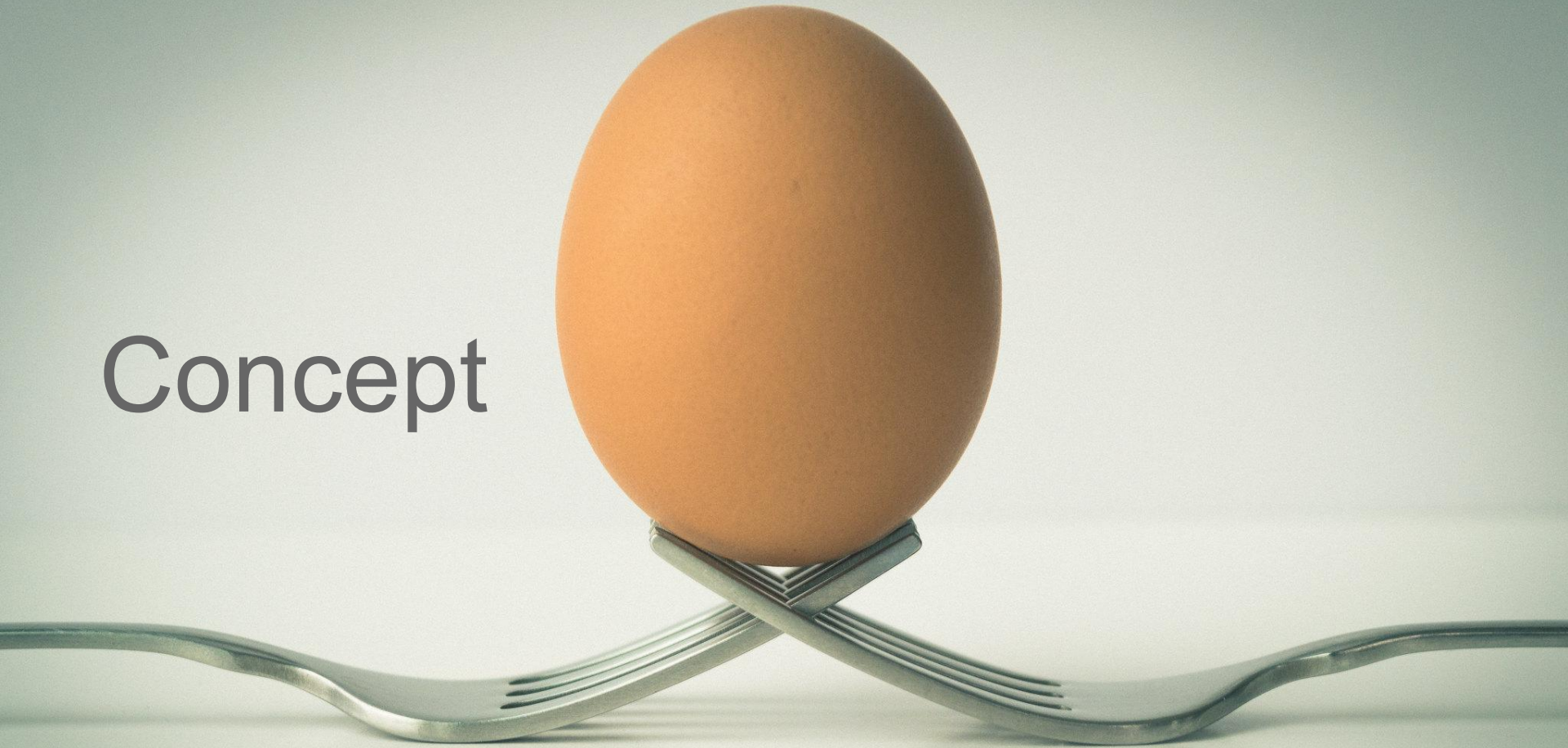


Figure 1: BeyondCorp components and access flow

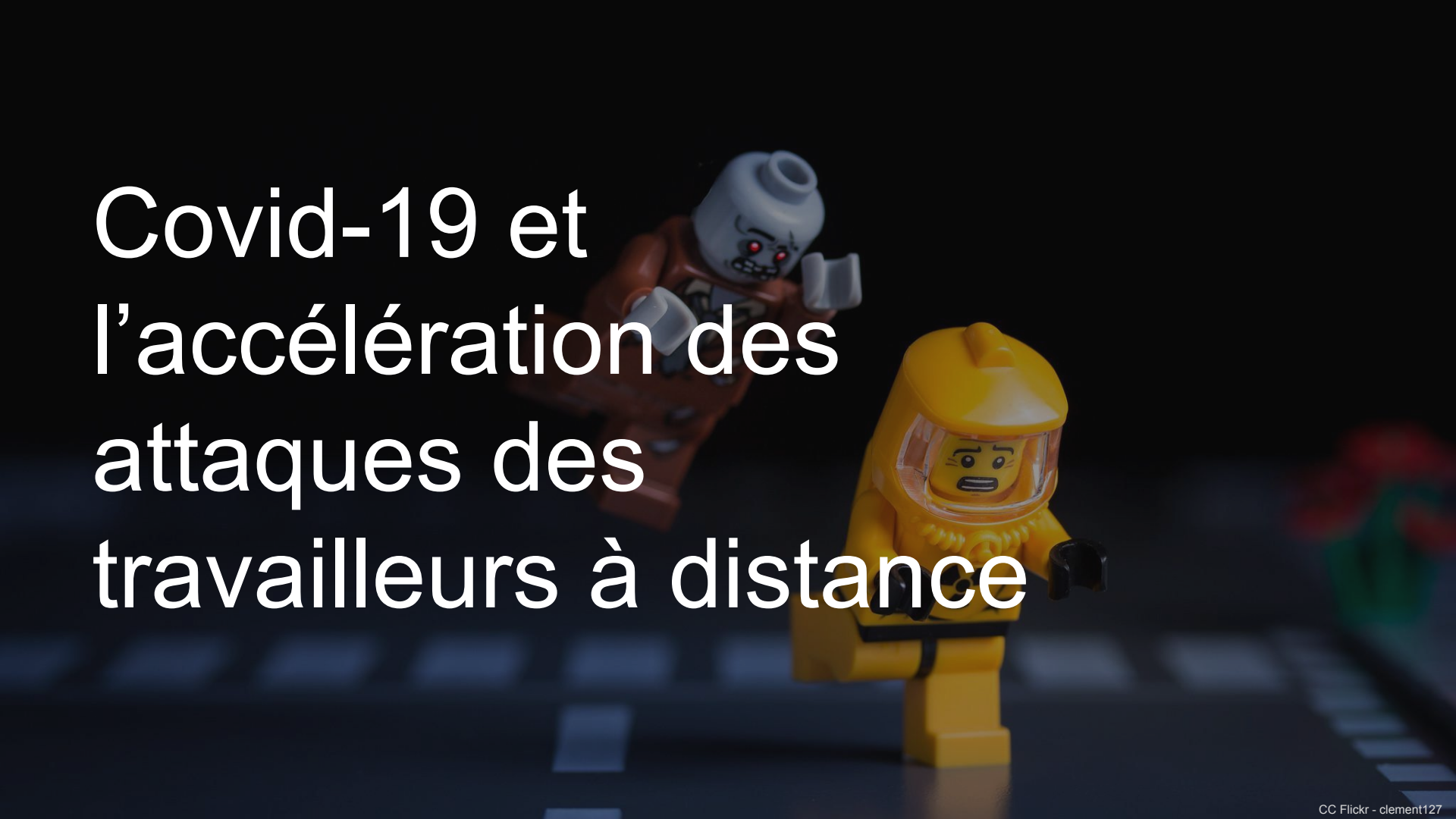
Concept



Covid-19 et l’accélération du travail à distance

CC Flickr - neilmoralee

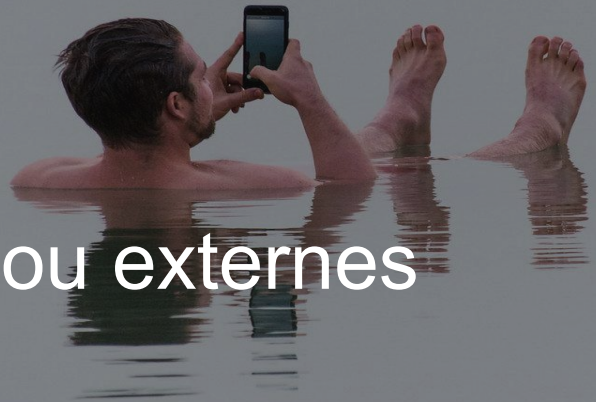
Covid-19 et l’accélération des attaques des travailleurs à distance



Les risques

Applications

- Mobiles
- Web
- Internes ou externes



Réseau sans-fil WiFi

CC Flickr - nenadstojkovic

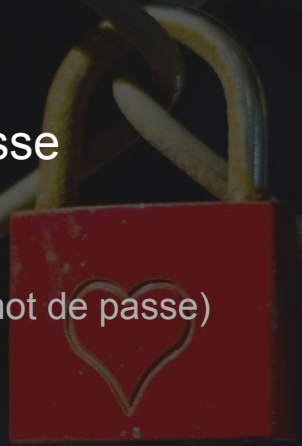
Matériel non conforme


Bonnes pratiques et mesures de sécurité

Concerne tout le monde

Recommendations

- Bon mot de passe (passphrase)
  - 16 et +
  - Si possible 25 à 100 de long
- Utilisation d'un gestionnaire de mots de passe
  - 3 mots de passe à se rappeler
    - Ordinateur
    - Courriel (email backup du gestionnaire de mot de passe)
    - Gestionnaire de mots de passe
- Bon mot de passe WiFi
- Ne partagez pas votre ordinateur de travail avec vos enfants et votre famille
- Sécurisez vos IoT (objects connectés) sur un réseau sans-fil d'invité et séparez de votre réseau personnel et d'emploi




Question?