

Télétravail et outils de collaboration

Comment les pirates vous ciblent aujourd'hui ?

Patrick Mathieu, Hackfest.ca

Octobre 2020

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: @patheti

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>



Infosec Jobs

<https://infosecjobs.ca>



HACKFEST.ca

GET
INVOLVED

info@hackfest.ca



DISCORD

<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

A hand holds a black and white photograph of a large crowd gathered for a protest or rally at the Washington Monument. The crowd is dense and extends far down the reflecting pool. The Washington Monument stands tall in the background. The photo is held up in front of a modern-day color photograph of the same location, showing a much sparser crowd of people walking on the steps and sitting on the grass. The text "D'hier à aujourd'hui" is overlaid in white on the black and white photo.

D'hier à aujourd'hui

Le passé - Le périmètre



Le passé c'était aussi la phrase:

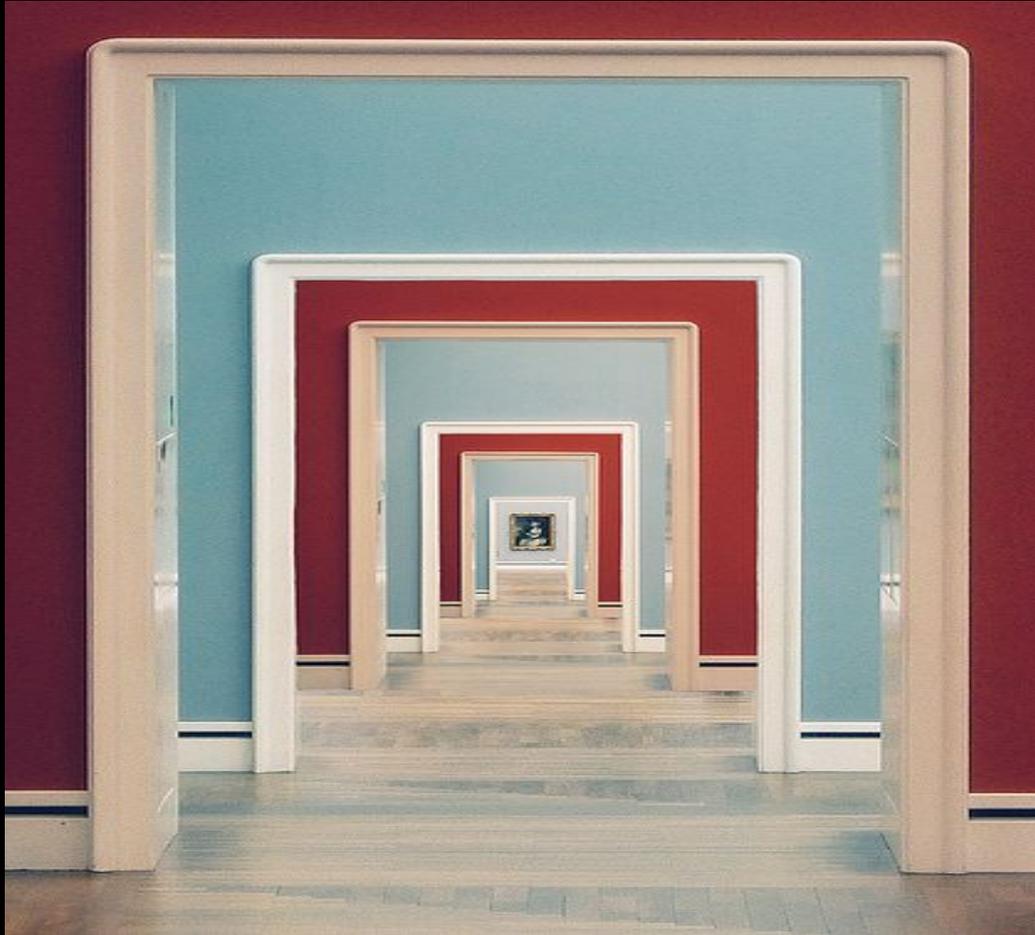
“Oui, mais on a un Firewall?”



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

SECURITY

présentation public

BeyondCorp: A New Approach to Enterprise Security

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

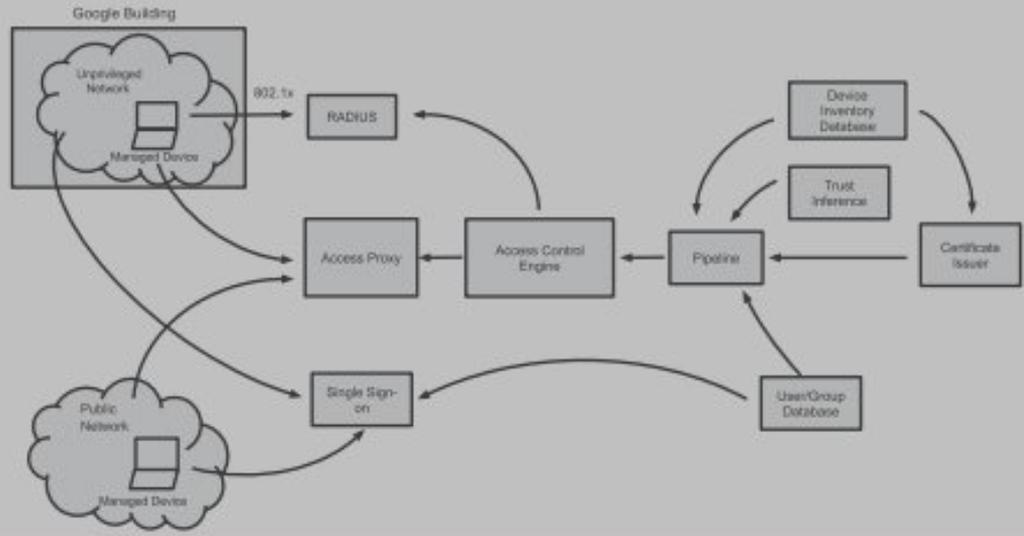
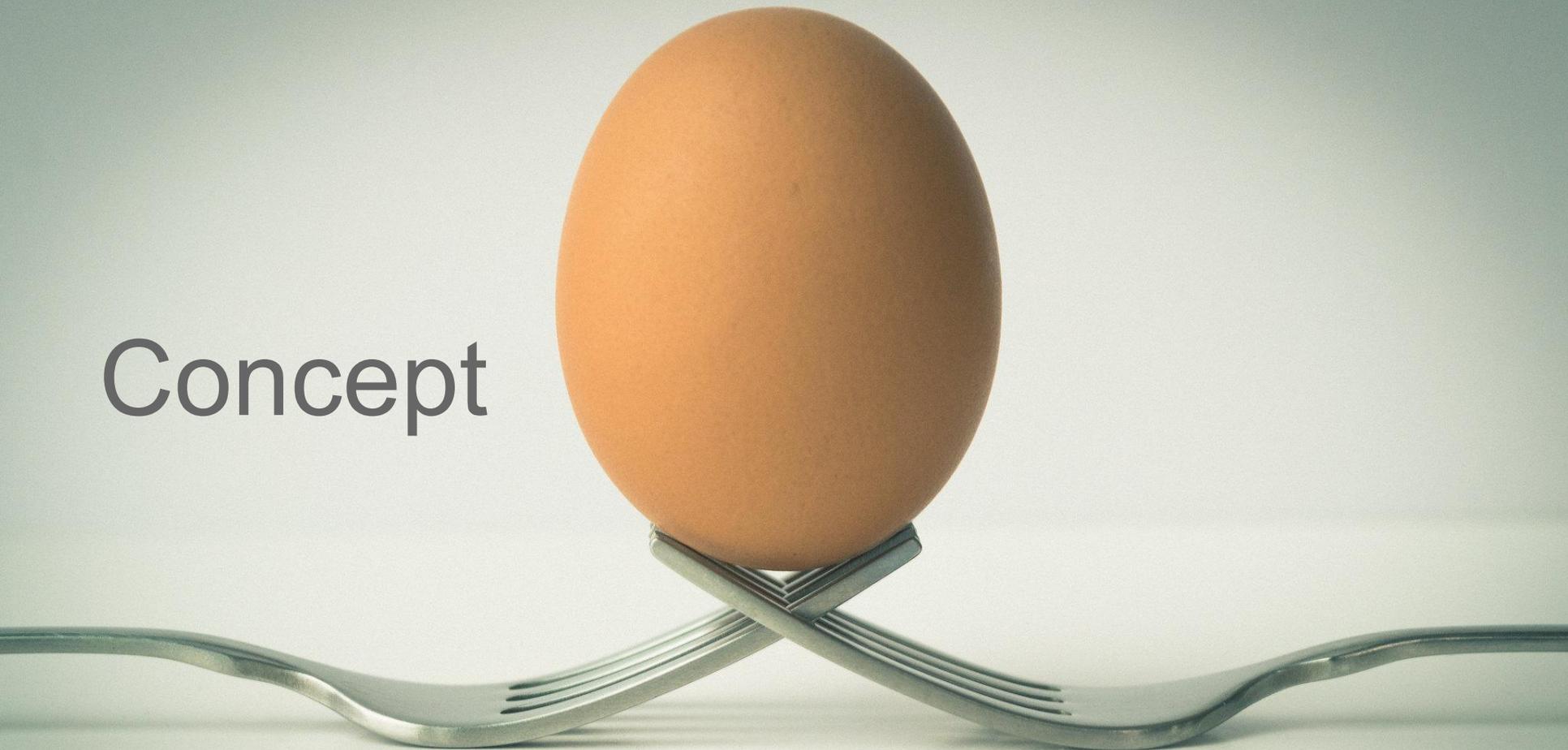


Figure 1: BeyondCorp components and access flow

Concept





Covid-19 et l'accélération du travail à distance

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



A person is captured in mid-air, jumping from a dark, rocky cliff on the left side of the frame. The person is silhouetted against a clear, bright blue sky. Below the cliff, a calm, blue lake stretches across the middle ground, reflecting the sky. In the background, a range of mountains with some snow patches is visible under the same clear sky. The overall scene conveys a sense of adventure and risk.

Les risques

Applications

- Mobiles
- Web
- Internes ou externes



Réseau sans-fil WiFi



A photograph of a woman and a young girl sitting on the floor in a living room, looking at a laptop screen. The woman is on the left, wearing an orange top, and the girl is on the right, wearing a white top with black polka dots. The background shows a couch and some toys on the floor. The text "Votre famille Et amis" is overlaid on the left side of the image.

Votre famille Et amis

Matériel non conforme





Bonnes pratiques et mesures de sécurité

A photograph of a busy city street at night. The scene is filled with pedestrians walking across a crosswalk. In the background, a large building with a distinctive diamond-patterned facade is brightly lit, featuring two prominent 'KKBOX' signs. To the left, a large, dark, rounded tree stands in front of a brightly lit storefront. The overall atmosphere is one of a vibrant, bustling urban environment.

Concerne tout le monde

Recommandations

- 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 (objets connectés) sur un réseau sans-fil d'invité et séparez de votre réseau personnel et d'emploi





Question?