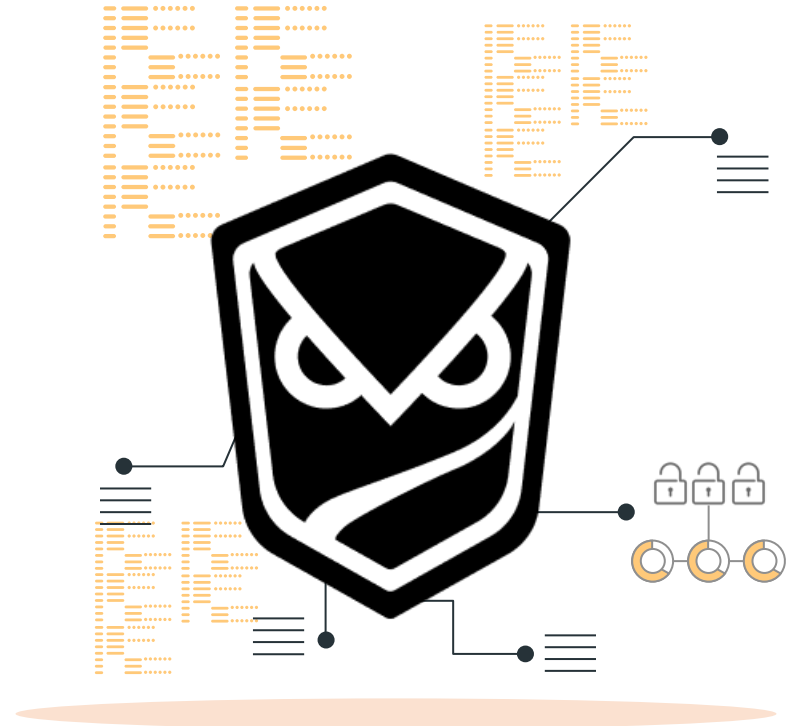


Démotiver les attaquants

Nouvelles menaces,
nouvelles stratégies



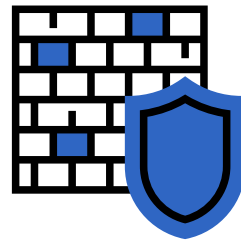
Avant Menaces Stratégies



Je vous parle d'un temps
que les moins de vingt ans
ne peuvent pas connaître...

... avant 2015

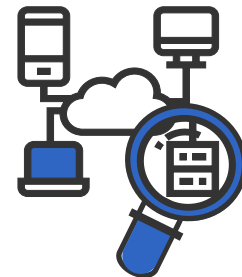
Avant Menaces Stratégies



Firewall



WAF



IDS/IPS



Antivirus

Avant Menaces Stratégies



Défense périmétrique



Défense en profondeur

Avant ~~Menaces~~ Stratégies

Changements



Cloud, SaaS, télétravail



Avant ~~Menaces~~ Stratégies

Changements



Cloud, SaaS, télétravail



Agile avec SCRUM



Changements tous les mois,
toutes les semaines

Avant ~~Menaces~~ Stratégies

Du neuf avec du vieux



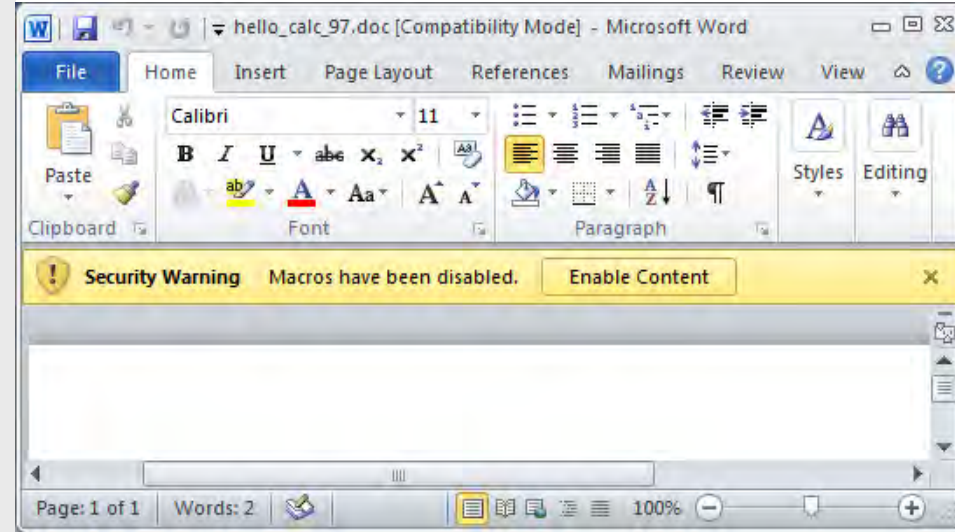
Cloud, SaaS, télétravail



Agile avec SCRUM



Macro Office



Microsoft désactivera les macros en avril 2022

Avant **Menaces** Stratégies



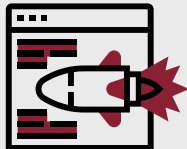
Cloud, SaaS, télétravail



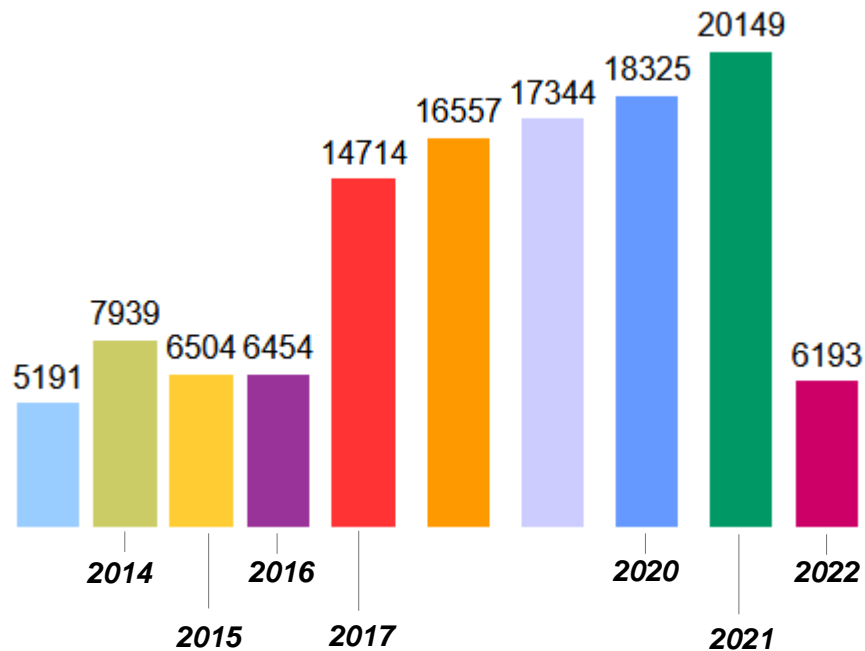
Agile avec SCRUM



Macro Office



2016: 6k vulns, 2021: 20k



Difficultés à suivre les menaces

Avant **Menaces** *Stratégies*



Cloud, SaaS, télétravail



Agile avec SCRUM



Macro Office



2016: 6k vulns, 2021: 20k



Business structuré



Avant *Menaces* ~~**Stratégies**~~

Avant



Avant

Menaces

Stratégies

En continu

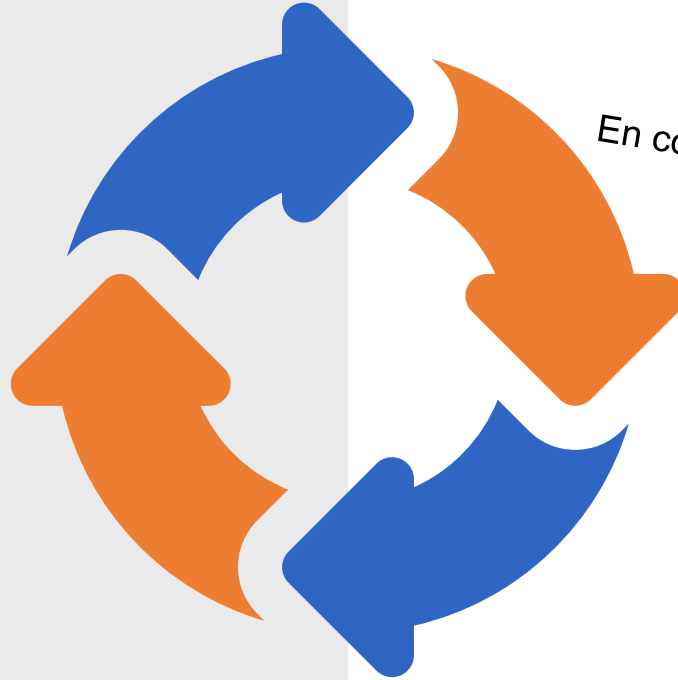
En continu

En continu

En continu

En continu

En continu



En continu

En continu

En continu

En continu

En continu

En continu

oui, je sais, c'est moche ;-)



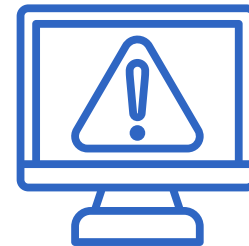
Prévention en continu

- > Scans internes
- > Cartographie externe (EASM)
- > Veille
- > Pentest (PTaaS)



Détection en continu

- > EDR
- > SOC



Réponse en continu

- > CERT / CSIRT
- > Hunting

Conclusion

Piratages

49%

Hameçonnage

- > *Exercices (mais pas trop)*
- > *Sécurisation du mail*
- > *Scans internes*

49%

Actif exposé sur internet

- > *Cartographie (en continu)*
- > *Pentests externes (en continu)*
- > *Veille (en continu)*

Vos contacts

Romaric GATTIN

✉ romaric.gattin@patrowl.io

☎ +33 (0)7 68 55 68 71



Vladimir KOLLA

✉ vladimir.kolla@patrowl.io

