aDvens

SECURITY FOR THE DIGITAL AGE

# QUAND 250 RSSI PARLENT DE SOC…

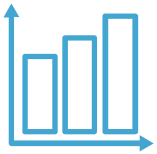
FIC Talk
22 Janvier 2019

# QUI SOMMES-NOUS ?

**1er pure-player français** de la cybersécurité, Advens vous accompagne pour prendre de l'avance et faire de la sécurité un actif différenciateur.

**180**

Collaborateurs à Paris, Lille, Lyon, Bordeaux & Nantes



**30%**

Croissance annuelle

**+300**

Clients actifs en France et à l'étranger

PALMARÈS Capital MEILLEUR CABINET DE CONSEIL 2019

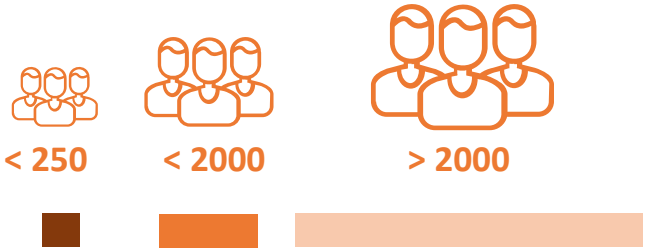
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMÉES

VISA DE SÉCURITÉ — ANSSI

Happy AT WORK — choose mycompany 2019 FRANCE — Happy Trainees

# 250, VRAIMENT ?

Une étude initiée grâce à la communauté du CESIN (500 membres)





## Novembre 2018

- Création d'un sondage sur le sujet du SOC
- Orientation retenue : liens entre SOC & Cyber-résilience
- 257 réponses collectées

## Décembre 2018

- Animation d'un atelier lors du congrès du CESIN
- Compléments et anecdotes

## Janvier 2019

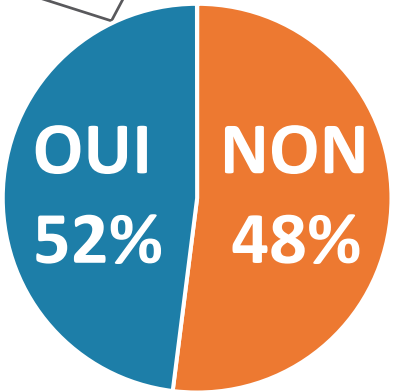
- Synthèse

# PREMIÈRES IMPRESSIONS

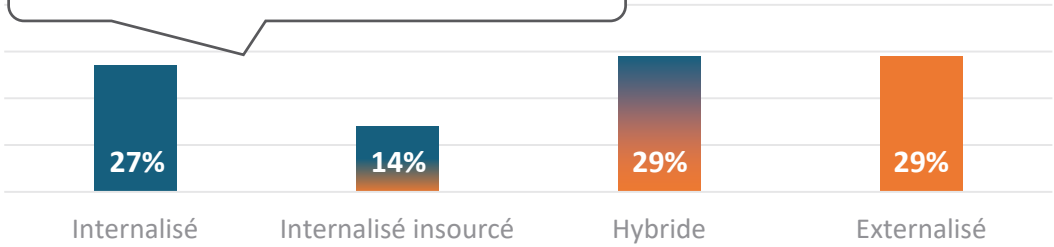
Comment pourriez-vous définir la relation entre votre SOC et vous ?....

- Célibataire
- En couple
- Marié
- C'est compliqué ✓
- Dans une relation libre

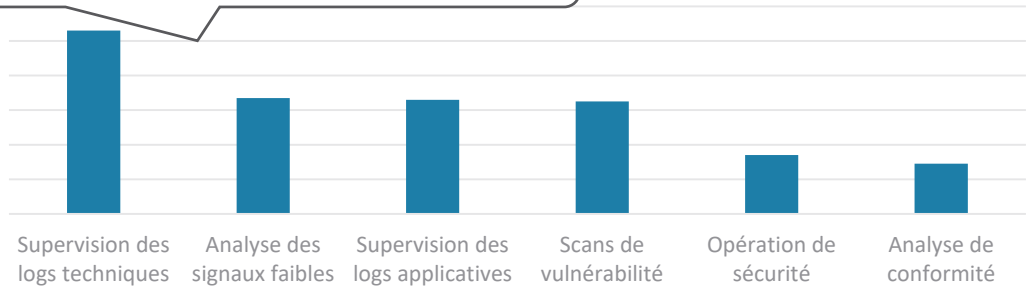
## Avez-vous un SOC ?




## Quel mode d'organisation ?




## Quels services proposés ?



# LA BONNE NOUVELLE ?

**79%**

**considèrent que le SOC renforce la capacité de cyber-résilience… Mais…**

# LES DIFFICULTÉS…

## #1 : Couverture du périmètre & Maitrise des risques Métier

*« Intégrer des use cases les plus proches des processus métiers »*

*« Une meilleure couverture »*

*« L'intégration de la composante métier »*

*« Prise en compte du domaine applicatif et des environnements digitaux (AWS, Azure) »*

✓ **Mettre sous surveillance l'ensemble des actifs**
✓ **Proposer une supervision des risques Métier**

# LES DIFFICULTÉS…

## #2 : Pertinence & Efficacité des alertes

*« Périmètre d'analyse, automatisation du premier niveau d'analyse »*

*« La pertinence des remontées Ajouts de logs Meilleure réactivité »*

*« Pertinence des alertes »*

*« Réduction des faux positifs avec l'apport du machine learning »*

✓ **Industrialiser la collecte et l'analyse**
✓ **Rendre les alertes plus pertinentes et plus rapides**

# LES DIFFICULTÉS…

## #3 : Réponse & Automatisation

*« Automatisation des réactions »*

*« Industrialiser les processus de remédiation »*

*« Amélioration des sources de logs, industrialisation de la gestion du premier niveau d'alerte, intégration MSSP pour approche hybride »*

✓ **Dépasser le stade de la détection**
✓ **Orchestrer la sécurité au quotidien**

# SECURITY-AS-A-SERVICE FACTORY

Conçue pour fabriquer, industrialiser et fournir des solutions Security-as-a-Service qui traitent de multiples cas d'usage pour relever le défi de la sécurité à l'ère numérique.

Une **plateforme AI-driven** propriétaire pour orchestrer l'ensemble des services

Un **centre opérationnel de sécurité** de plus de 50 experts regroupant toutes les compétences pour prévenir, détecter, réagir et protéger

Une **méthodologie agile** orientée « Cas d'usage » pour adresser vos périmètres et enjeux essentiels

# SECURITY-AS-A-SERVICE FACTORY

- **1,5 milliard d'évènements collectés par jour**
- **+500 règles et algorithmes testés et déployés en production**
- **Silicon Cybersecurity Awards**
  Meilleure utilisation de l'IA dans une solution de sécurité
- **Services déjà opérationnels**
  SOC-as-a-service, Conformité-as-a-service, Technology-as-a-service
  Plus de 50 clients
  Service international et 24/7
- **Qualification PDIS en cours**
- **Nombreuses contributions à l'écosystème OpenSource**

aDvens
SECURITY FOR THE DIGITAL AGE

advens.fr

*Paris +33 1 84 16 30 25*
*Lille +33 3 20 68 41 81*
*Lyon +33 4 28 29 08 29*
*Bordeaux +33 5 35 54 82 84*