

**Comment décider si les solutions logicielles
libres ou commerciale conviennent le mieux
à vos besoins**

S·Q·A·LOGIC



Sponsorisé par

**MICRO
FOCUS®**

Agenda

- **QUI SOMMES-NOUS?**
 - Micro Focus
 - SQALogic
 - Les Présentateurs
- **La croissance de l'Open Source**
- **Mythes vs Réalités**
- **Différences entre les coûts Open Source et les coûts des logiciels commerciaux**
- **La transformation en cours**
- **Qualité et interopérabilité**
- **Formation**
- **Flexibilité**
- **Sécurité**
- **Fin**



Qui est Micro Focus?



Optimisation

Transformation numérique

Micro Focus fournit la **vitesse**, l'**agilité**, la **sécurité** et les **informations** requises pour réussir dans un secteur en pleine évolution.

Les **quatre piliers de base** de la transformation numérique



DevOps d'entreprise



Gestion de l'informatique hybride



Sécurité, risques et gouvernance



Predictive Analytics

Qui est SQA Logic?

- ✓ Fondé en 2012, avec un PDG de 25 ans d'expérience en assurance qualité
- ✓ Présence au Canada (Québec, Ontario)
- ✓ Présence aux États-Unis (NC)
- ✓ Réseau d'experts globaux passionnés en assurance qualité
- ✓ L'expertise d'un membre, les connaissances d'un groupe.

Présentateurs

David Milette

Fondateur et PDG

- Plus de 20 ans d'expérience dans le domaine de l'assurance qualité, occupant divers postes dans la gestion ainsi que d'être un implémenteur, intégrateur et consultant avant-vente avec des compétences de niveau architecte.
- Spécialisé dans les domaines de la gouvernance informatique, de la livraison des applications et de la gestion des applications qui sont connus sous le nom de BTO (Business Technology Optimization).
- Expert en méthodologies (DevOps, Agile, BDD, etc.), en solution logiciel pour l'Assurance Qualité (SQA) et ERP / CRM, en configuration des systèmes productions et de test, ainsi que l'automatisation des tests.



Présentateurs

Luigi Iuliani

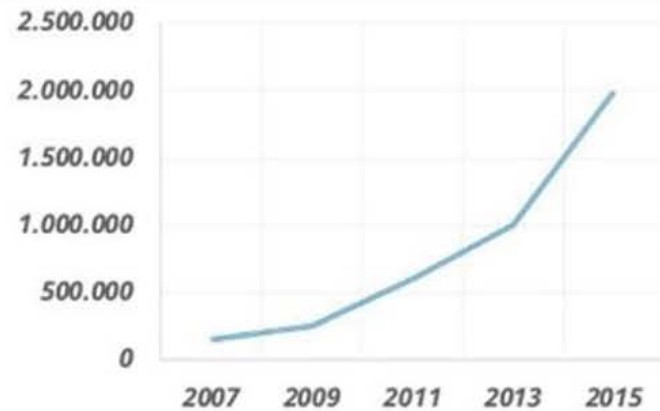
Architecte de processus et de solution - DevSecOps

- Plus de 18 ans d'expérience dans la définition, l'architecture et la mise en œuvre d'applications / outils logiciels, de gestion de configuration logicielle et de processus de développement SEI-CMM / IEEE
- Spécialisé dans les systèmes autonomes (voitures et drones) ING., FinTech, DevSecOps, BlockChain, Intelligence artificielle, Machine Learning, Agritech, Big Data-AR et plus encore.
- Certifié avec de nombreuses technologies, méthodologies et meilleures pratiques de l'industrie.



Open Source est en croissance exponentielle

Croissance des projets Open Source



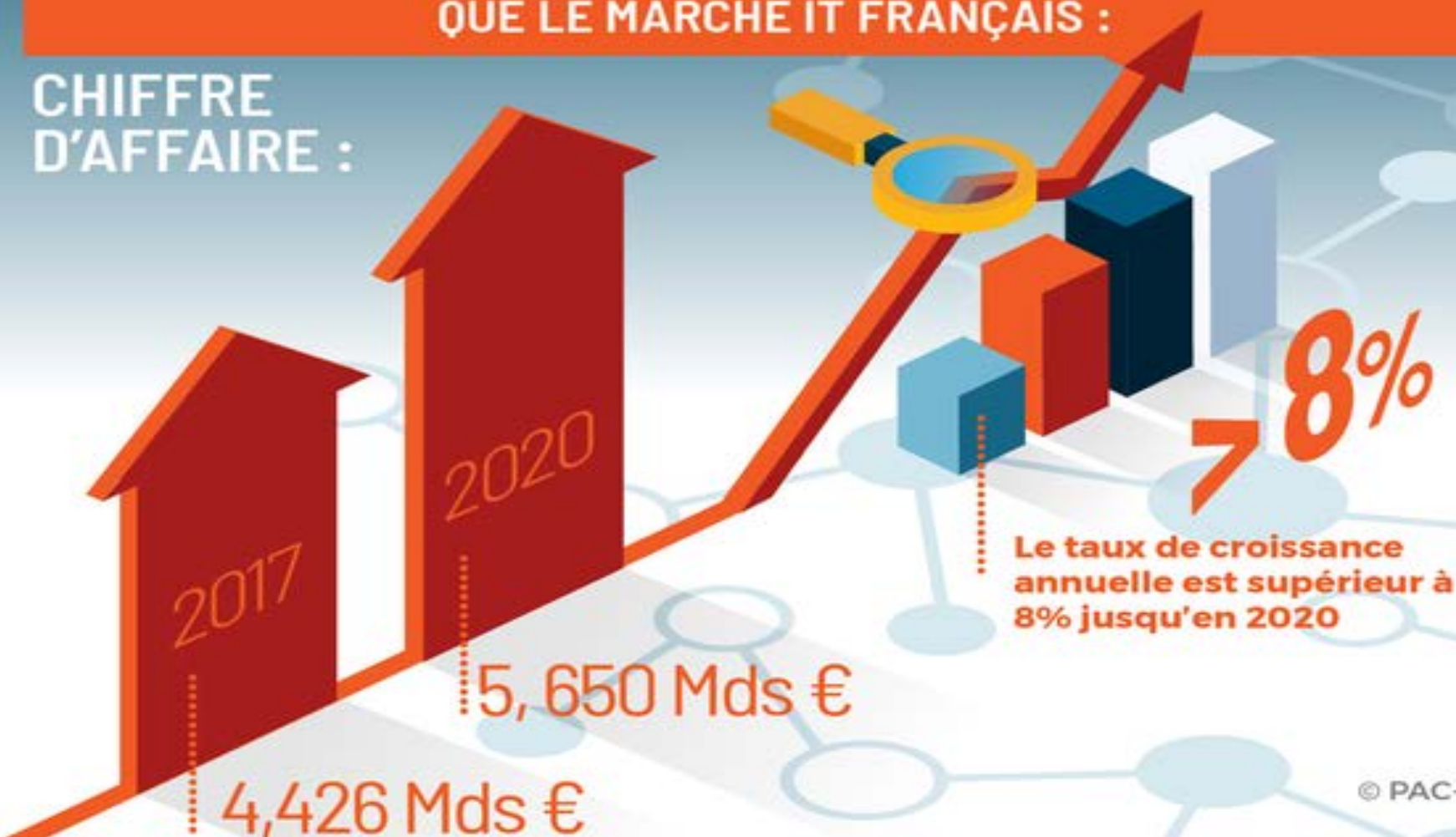
Source: Black Duck Management Webinar 2014

Tendances de l'emploi openstack



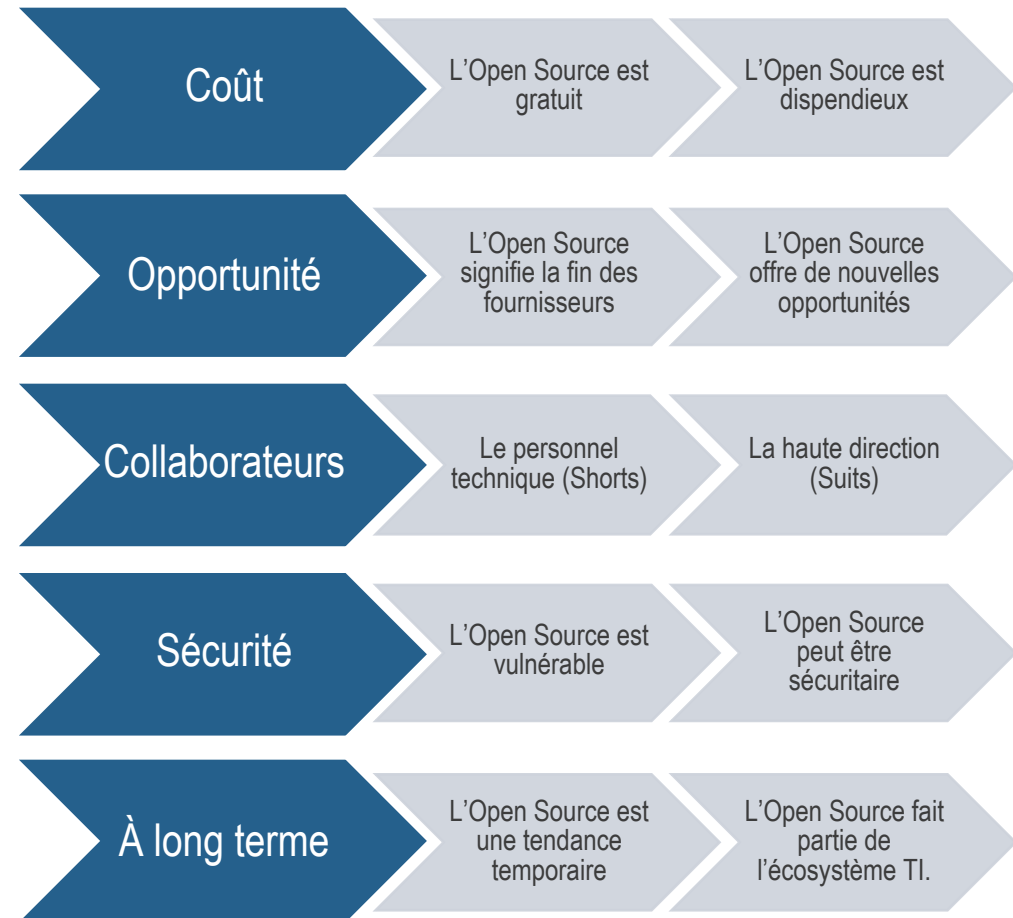
L'OPEN SOURCE, UN MARCHÉ 2 FOIS PLUS DYNAMIQUE QUE LE MARCHÉ IT FRANÇAIS :

CHIFFRE
D'AFFAIRE :

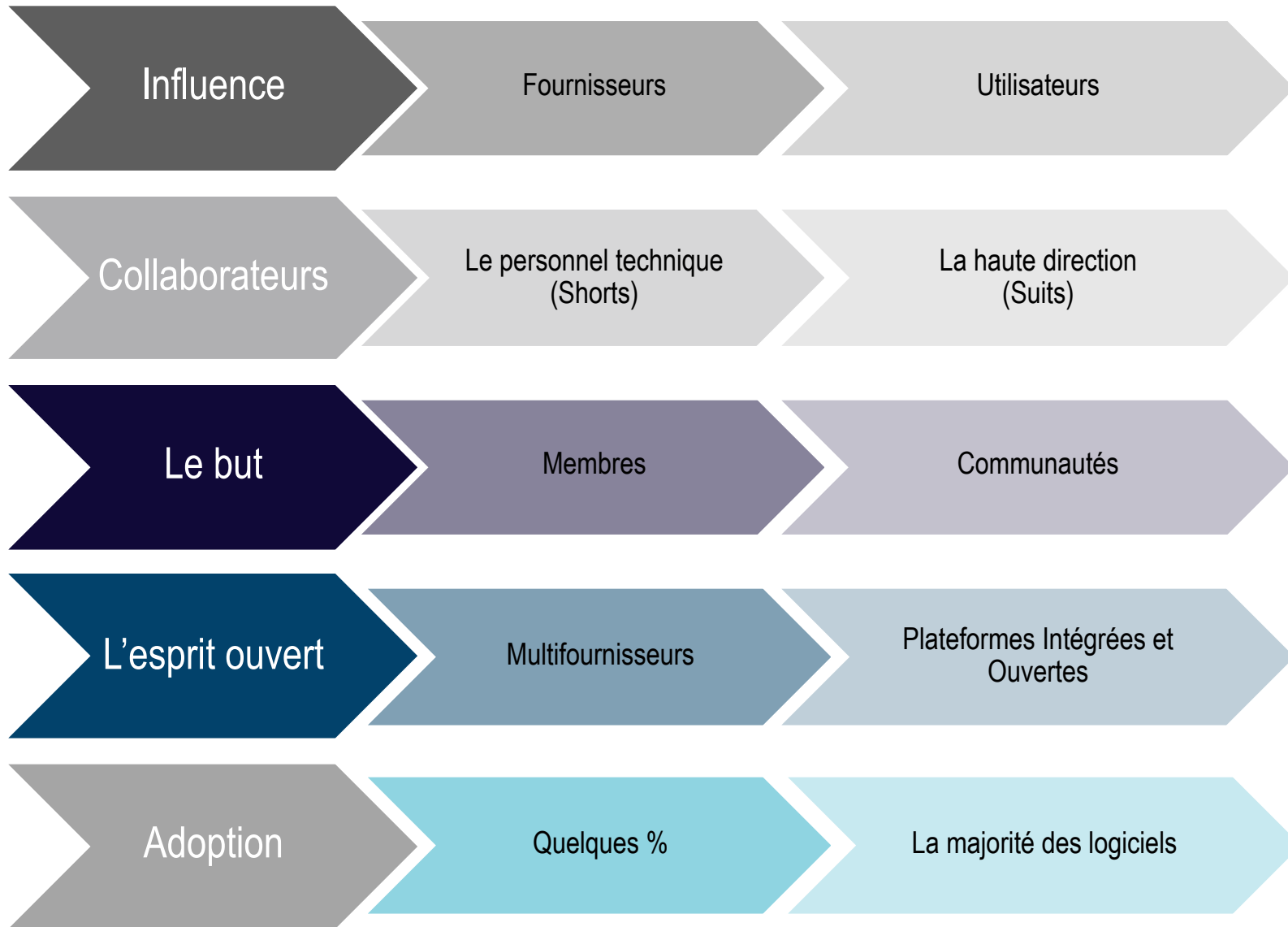




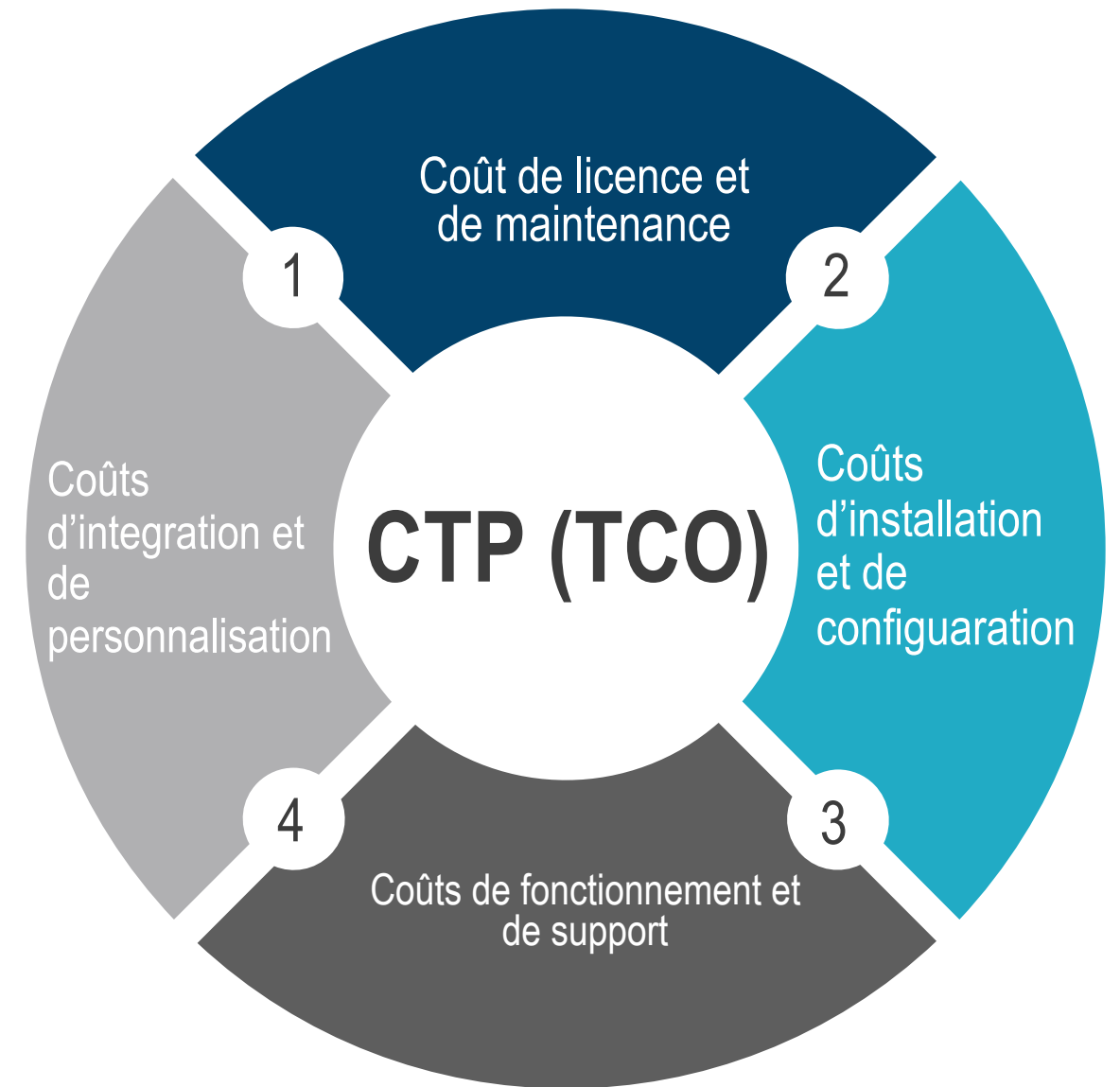
Open Source – Mythes vs Réalités



Une transformation est en cours!



Les différences entre les coûts Open Source et les coûts des logiciels commerciaux



Qualité et Interopérabilité



1. Robustesse



2. Assiduité



3. Intégrations



4. Support

Formation

- Offerte par le fournisseur vs dirigé par la communauté
- Formelle vs informelles
- Dirigé dans une classe vs en ligne
- Dispendieux vs abordable
- Certification officielle vs reconnaissance pairs



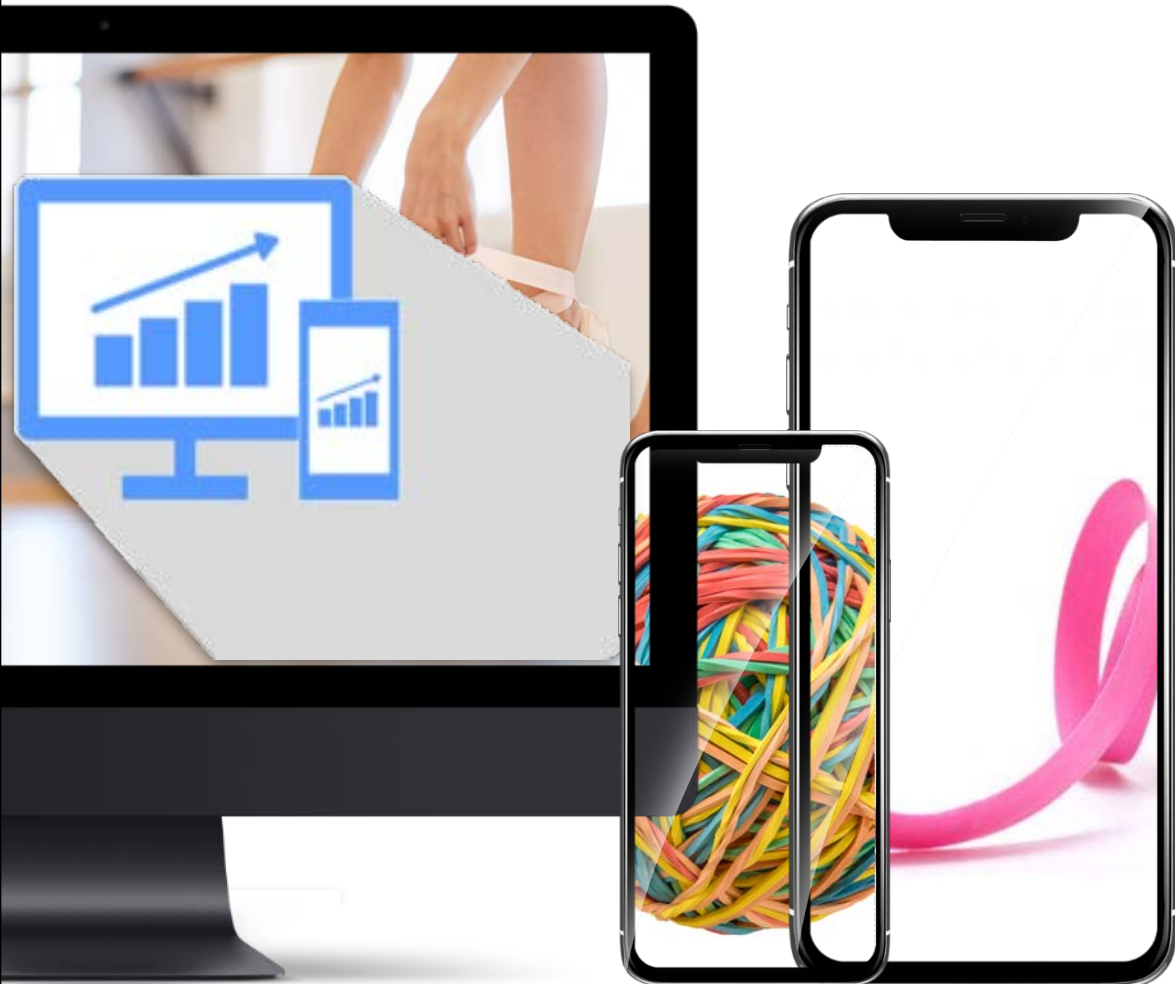
Flexibilité

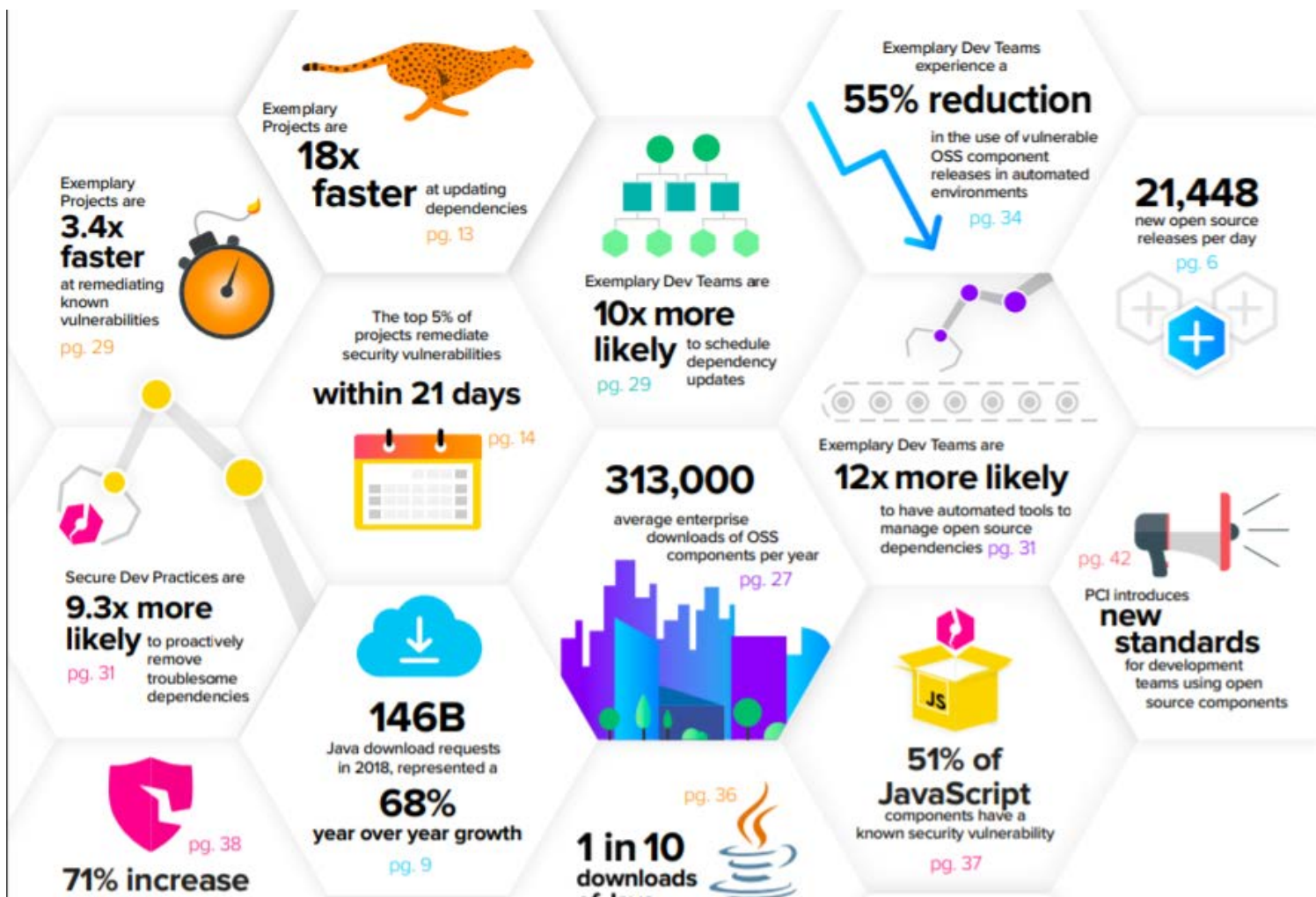
Open Source

- Nombreuses intégrations dues à l'implication de la communauté
- Code open source permettant des intégrations personnalisées
- Un niveau absolu de flexibilité dépendant du temps, de \$\$\$ et des efforts.
- L'apport de la communauté étendue stimule l'innovation (Bleeding edge)

Commercial

- Intégrations solides et robustes avec la suite des fournisseurs
- Alignés sur meilleures pratiques d'industrie et la vision du marché
- Développement suivant les visions des leaders d'industrie
- Adeptes éprouvés et fidèles des meilleures pratiques de l'industrie





«Cependant, avec des recherches montrant que 78% des bases de code auditées contenaient au moins une vulnérabilité open source, dont 54% étaient des vulnérabilités à haut risque que les pirates pourraient exploiter, il existe des preuves claires que l'utilisation de code open source comporte des risques de sécurité. De tels risques ne surviennent souvent pas en raison de la qualité du code open source (ou de son absence) mais en raison d'une combinaison de facteurs impliquant la nature du modèle open source et la façon dont les organisations gèrent leurs logiciels.

Un exemple pertinent de problèmes dus à des exploits accessibles au public a été la principale violation d'Equifax en 2017, dans laquelle l'agence d'évaluation du crédit a dévoilé les données personnelles de 143 millions de personnes. La raison primaire pour laquelle l'exposition s'est produite est que les attaquants ont remarqué qu'Equifax utilisait une version du framework open source Apache Struts qui présentait une vulnérabilité à haut risque, et les pirates ont utilisé ces informations à leur avantage. »

Processus de traitement d'incidents de Sécurité

Response Center Procedures

The Response Center has established an efficient process aligned with industry best practices to ensure that each potential security incident or vulnerability will be addressed, evaluated and communicated internally within Micro Focus in a timely manner in order to prepare a clear resolution plan.

1. Preparation

- Receiving notification
- Collecting relevant data
- Communication to relevant Micro Focus parties

2. Analysis & investigation

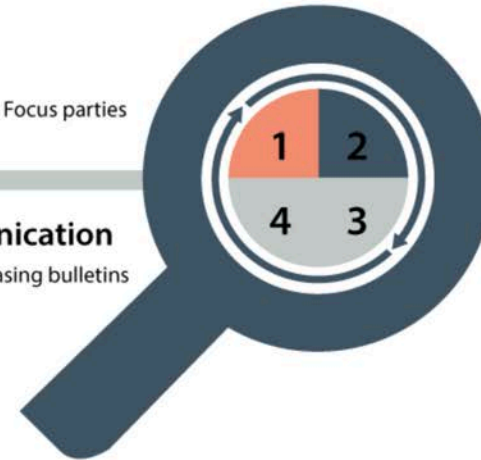
- Reproduce potential vulnerability
- Risk evaluation
- Correlation to other products

4. Resolution & communication

- Communication resolution & releasing bulletins
- Conclusion & constant improving

3. Containment & recovery

- Establish solution strategy
- Generating optimal & efficient resolution
- Approving solution



Accelerate delivery pipeline with MF Enterprise DevOps - Workflow

