Expertise technique en sécurité informatique

Expertise technique en sécurité informatique

Sommaire

Expertise technique en sécurité informatique

Sommaire

COGICEO

Expertise technique en sécurité informatique

Identité

- Société indépendante
- Expertise technique en sécurité informatique
- Consultants avec plus de 8 ans d'expérience
- Orateurs et sponsors d'événements nationaux (CRIP, NSC, OSSIR, SSTIC)
- Certifiés Instructeurs SANS depuis 2013
- Certifiés PASSI depuis 2016

Cogiceo

Expertise technique en sécurité informatique

Services

Audit

- A1. Test d'intrusion
- A2. Audit de configuration
- A3. Audit d'architecture
- A4. Audit organisationnel et physique
- A5. Audit de code source

Protection

- P1. Assistance technique responsable sécurité
- P2. Intervention d'urgence pour diagnostic

Formation

- F1. Sensibilisation COMEX/CODIR/DSI
- F2. Formation administrateurs Windows
- F3. Formation développeurs

SaaS

- S1. Cogiceo-Explorer : analyse de surface d'exposition internet
- S2. Cogiceo-ADanalyser : analyse de domaines Microsoft

Expertise technique en sécurité informatique

Sommaire

Définition

Dans l'environnement de réseau Microsoft, la notion de domaine définit un ensemble de machines partageant des informations d'annuaire.

Le domaine est composé de 5 éléments :

1. L'annuaire Active Directory
2. Les contrôleurs de domaine
3. Les serveurs
4. Les postes clients
5. Les relations d'approbations entre domaines

Compromission

La compromission d'un domaine permet l'accès aux :

- applications supportées par les serveurs
- applications dont l'authentification repose sur l'AD
- bases de données supportées par les serveurs
- bases de données dont l'authentification repose sur l'AD
- documents confidentiels présents dans les partages communs
- documents confidentiels présents sur les postes de travail
- postes de travail VIP pour déposer des outils d'espionnage
- plusieurs milliers de machines pour construire un botnet

COGICEO

Expertise technique en sécurité informatique

Constatations

- La compromission d'un domaine peut démarrer par un simple phishing
- 100% des tests d'intrusion internes mènent à la compromission du domaine
- Il faut généralement moins de 6h pour prendre le contrôle du domaine à partir d'une prise réseau ou d'une machine compromise
- Il est rarement nécessaire de faire un scan de ports/services, les IDS détectent ainsi peu la compromission du domaine
- Les SOC sont encore pauvres sur les méthodes classiques et ne mettent donc que peu en lumière les tentatives de compromission

Constatations

- La gestion de privilèges d'un compte n'est pas assez fine dans les organisations
- Les paramétrages par défaut priorisent la compatibilité au détriment de la sécurité
- La bonne ergonomie/flexibilité d'exploitation d'un domaine ne nécessite que peu de compétences, sa sécurité en revanche en demande nettement plus
- L'hyperconnectivité des filiales d'un groupe permet souvent la compromission de l'ensemble à partir de la prise de contrôle d'un seul domaine

Expertise technique en sécurité informatique

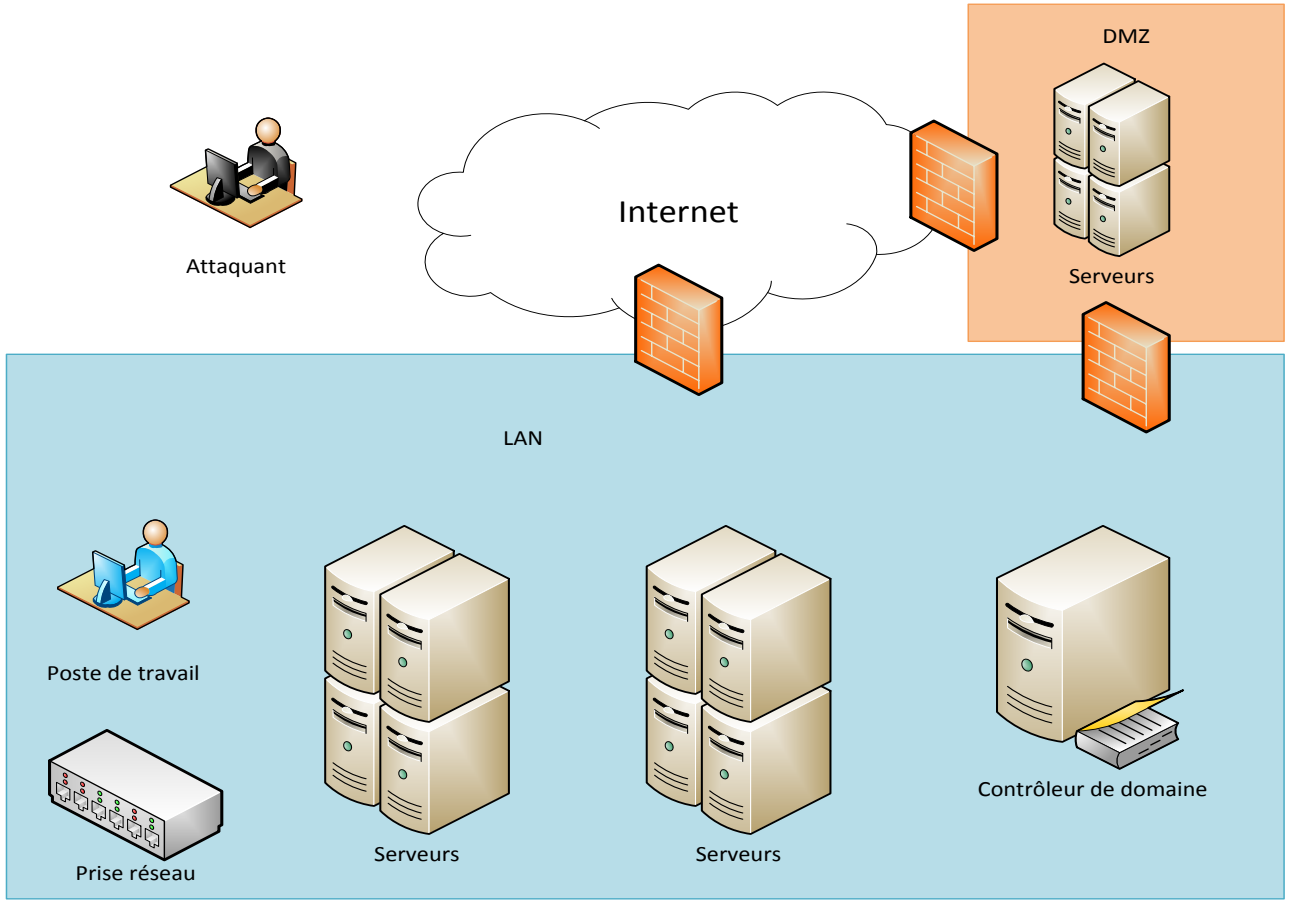
Sommaire

COGICEO

Expertise technique en sécurité informatique

Chemins de compromission classiques

Insertion dans le réseau → Compromission d'un compte sans privilège → Compromission d'une machine → Rebond sur d'autres machines → Compromission d'un compte à privilèges → Rebond sur d'autres machines → Compromission d'un compte admin du domaine



COGICEO

Expertise technique en sécurité informatique

Chemins de compromission classiques

Insertion dans le réseau → Compromission d'un compte sans privilège → Compromission d'une machine → Rebond sur d'autres machines → Compromission d'un compte à privilèges → Rebond sur d'autres machines → Compromission d'un compte admin du domaine

- Intrusion physique par effraction
- Intrusion physique sur invitation par Social Engineering
- Intrusion logique par phishing d'utilisateur via un mail ou une clé USB
- Intrusion logique par Social Engineering
- Vulnérabilités logicielles sur serveur exposé sur Internet
- Comptes triviaux ou par défaut sur service exposé sur Internet
- Défauts de cloisonnement entre la DMZ et le LAN

COGICEO

Expertise technique en sécurité informatique

Chemins de compromission classiques

Insertion dans le réseau | **Compromission d'un compte sans privilège** | Compromission d'une machine | Rebond sur d'autres machines | Compromission d'un compte à privilèges | Rebond sur d'autres machines | Compromission d'un compte admin du domaine

- Récupération de la construction de l'identifiant par meta-données (Metagoofil)
- Récupération de la liste des comptes sur LinkedIn (theHarvester)
- Récupération de la liste des comptes par connexion anonyme sur DC
- Phishing d'utilisateur via mail ou clef USB
- Social Engineering sur un utilisateur
- Bruteforce avec des mots de passe faibles
- Demande d'authentification via protocole de nommage secondaire (Responder)
- Man-In-The-Middle sur les phases d'authentification (Ettercap)
- Récupération du contenu du trousseau de clefs des navigateurs Internet

COGICEO

Expertise technique en sécurité informatique

Chemins de compromission classiques

Insertion dans le réseau → Compromission d'un compte sans privilège → **Compromission d'une machine** → Rebond sur d'autres machines → Compromission d'un compte à privilèges → Rebond sur d'autres machines → Compromission d'un compte admin du domaine

- Accès physique à la machine (disque non chiffré, DMA)
- Bruteforce de compte de base de données, d'applications
- Rejeu des comptes sans privilège sur les serveurs
- Rejeu des comptes sans privilège sur une ferme Citrix
- Vulnérabilité logicielle sur serveur exposé en interne
- Exploit sur un système d'exploitation non patché
- Elévation de privilèges locaux (PowerUp, Hot Potato)

COGICEO

Expertise technique en sécurité informatique

Chemins de compromission classiques

Insertion dans le réseau → Compromission d'un compte sans privilège → Compromission d'une machine → **Rebond sur d'autres machines** → Compromission d'un compte à privilèges → Rebond sur d'autres machines → Compromission d'un compte admin du domaine

- Défaut de cloisonnement et absence de réseau d'administration
- Rejeu de mot de passe et de hash
- Lecture des fichiers de configuration et de scripts
- Récupération de mots de passe dans les fichiers sysprep et unattend
- Recherche de mots-clés dans les partages
- Rejeu de ticket Kerberos

Chemins de compromission classiques

- Lecture des fichiers de configuration et de script
- Lecture des fichiers Group Policy Preferences (cpassword)
- Récupération de hash chiffrant le Ticket Granting Service (Kerberoast)
- Récupération de hash MsCache
- Récupération des comptes de taches planifiées et de services
- Rejeu de compte admin de domaine trust externe

COGICEO

Expertise technique en sécurité informatique

Chemins de compromission classiques

Insertion dans le réseau → Compromission d'un compte sans privilège → Compromission d'une machine → Rebond sur d'autres machines → Compromission d'un compte à privilèges → Rebond sur d'autres machines → **Compromission d'un compte admin du domaine**

- Vulnérabilité logicielle sur DC exposé en interne (MS14-068)
- Dump de la mémoire du processus LSASS (Mimikatz minidump)
- Modification de son Ticket Granting Ticket (SID history)

Expertise technique en sécurité informatique

Sommaire

COGICEO

Expertise technique en sécurité informatique

Video de compromission

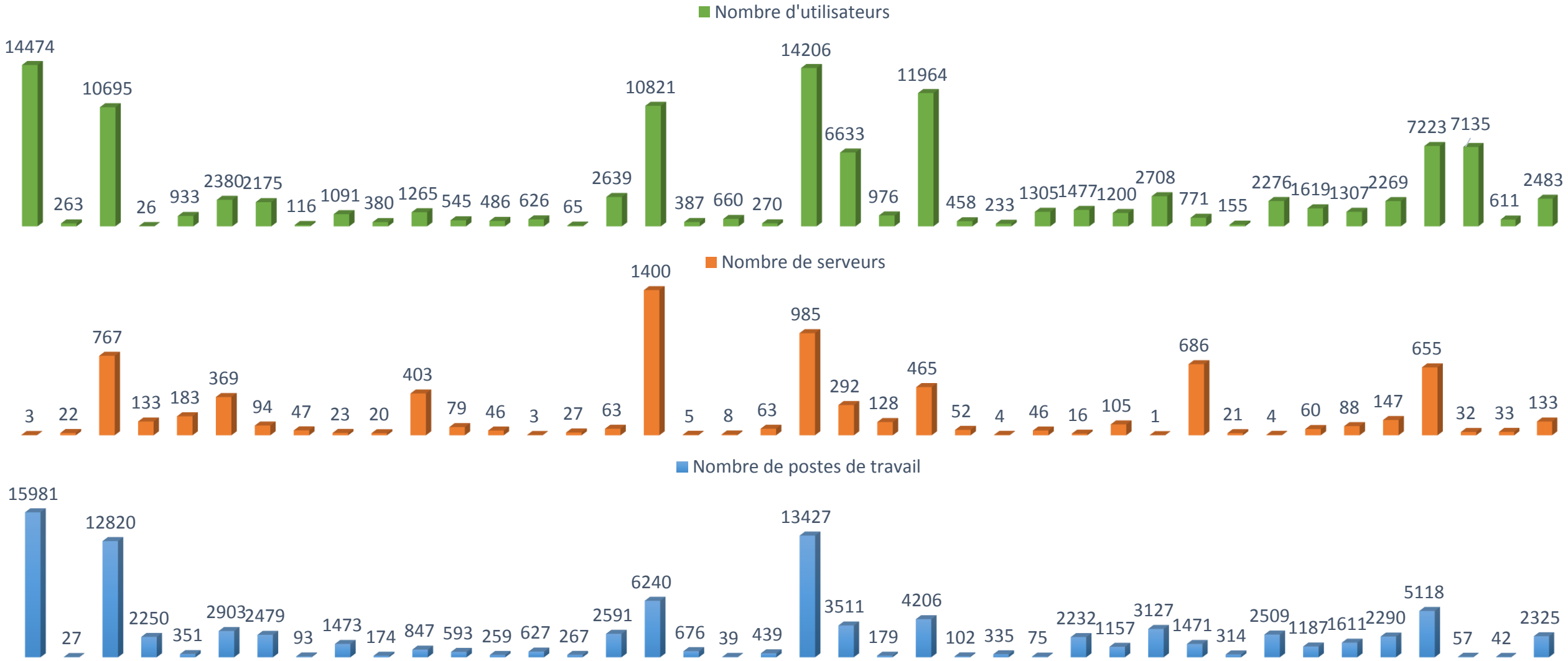
Expertise technique en sécurité informatique

Sommaire

COGICEO

Expertise technique en sécurité informatique

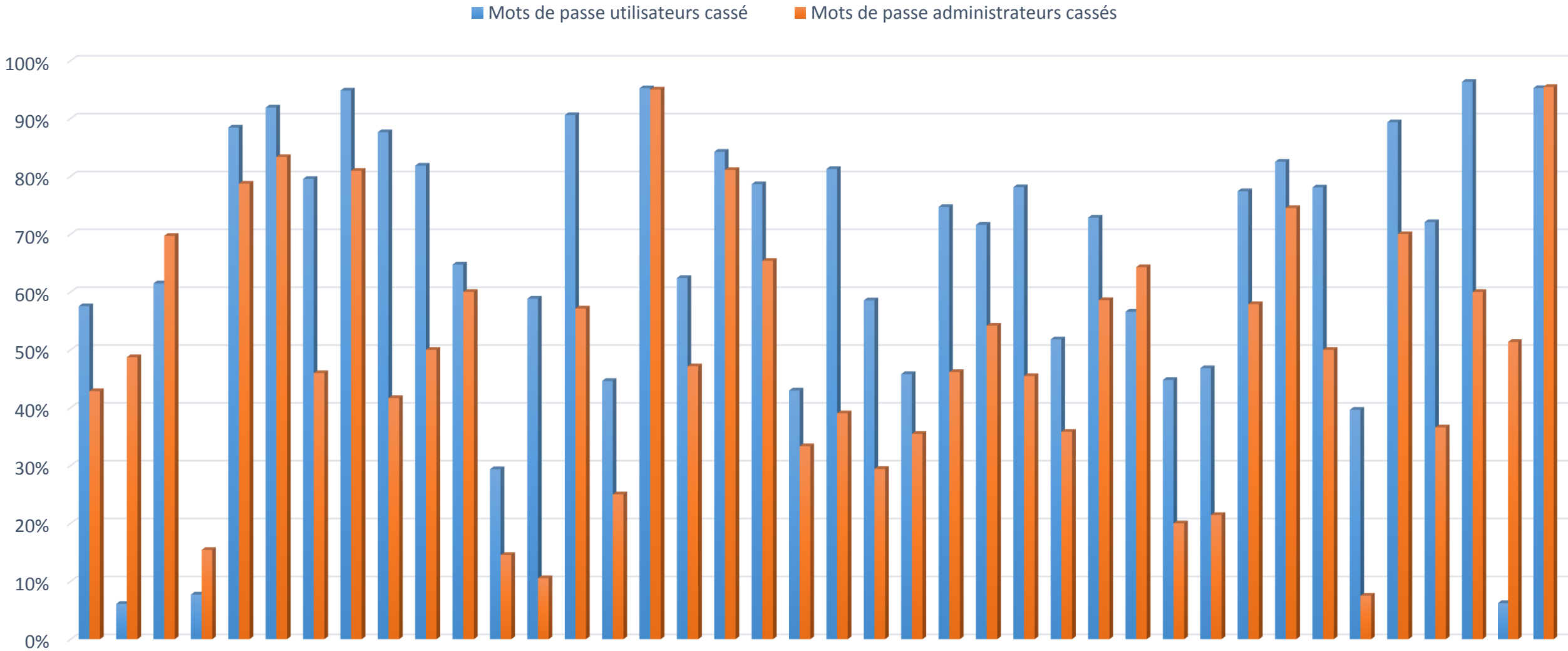
Nombres de machines



COGICEO

Expertise technique en sécurité informatique

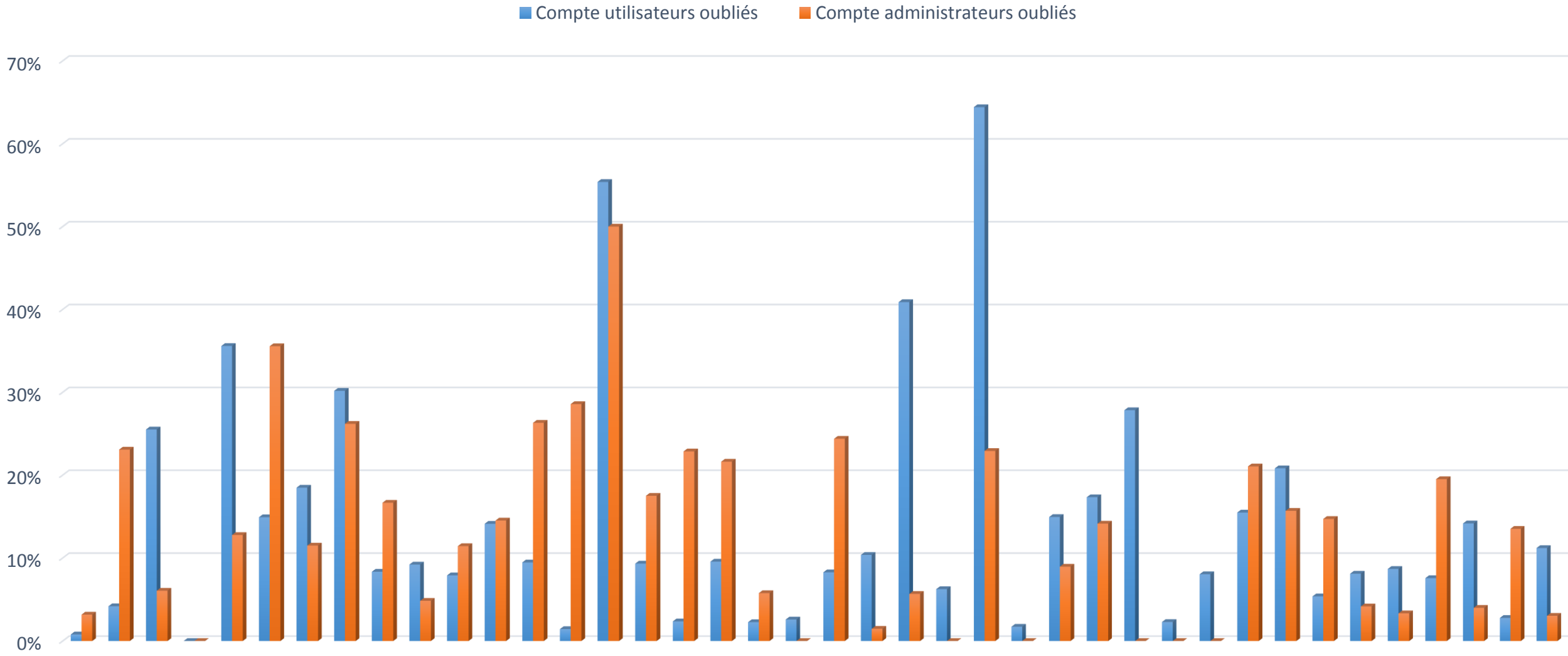
Mots de passe crackés



COGICEO

Expertise technique en sécurité informatique

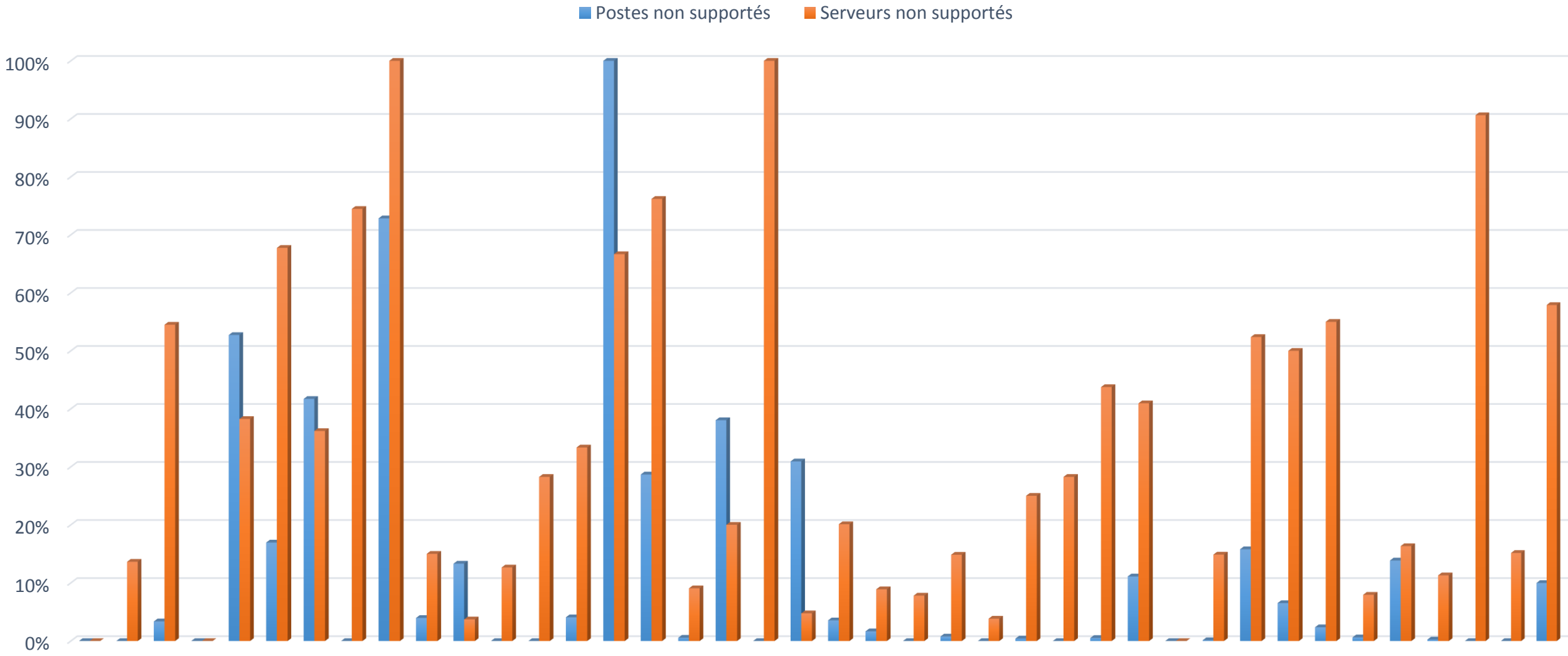
Comptes oubliés
(non connectés depuis +13 mois)



COGICEO

Expertise technique en sécurité informatique

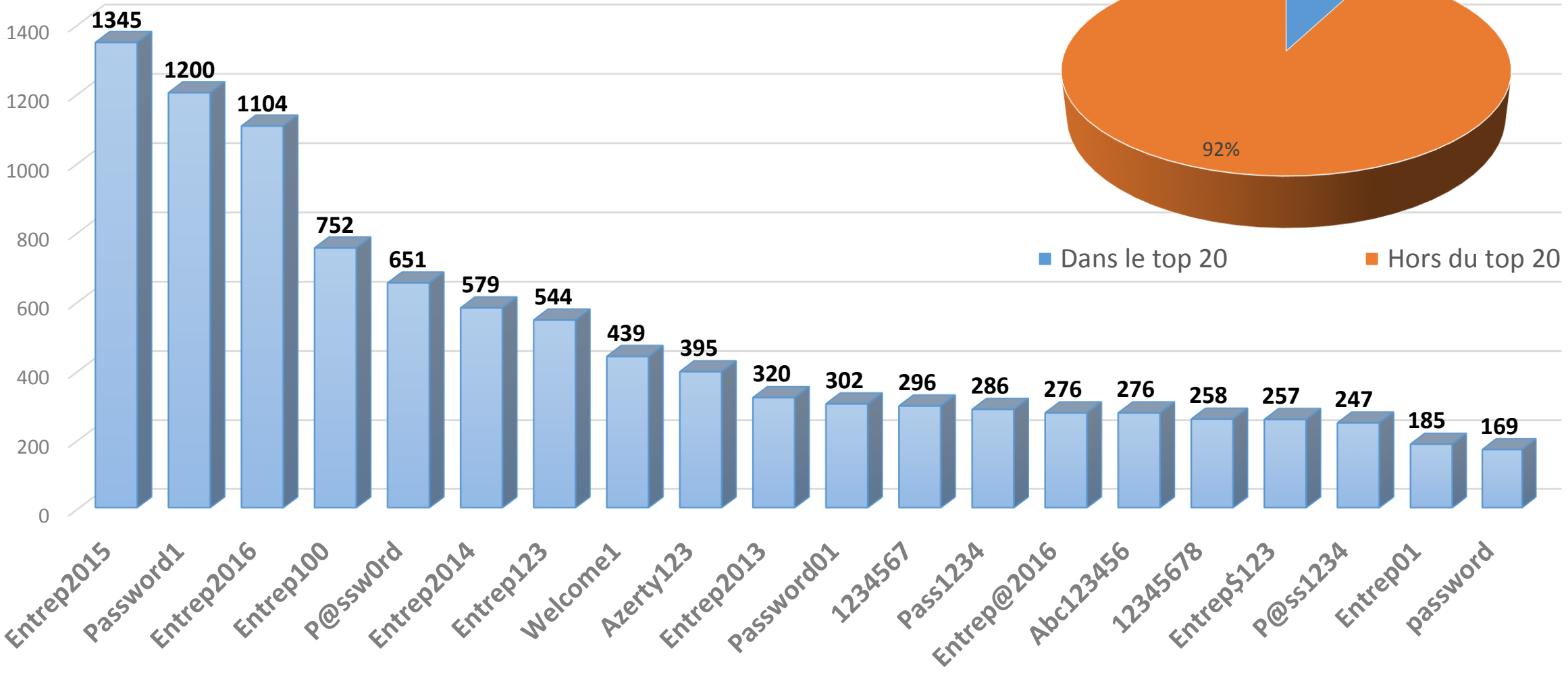
Machines non supportées



COGICEO

Expertise technique en sécurité informatique

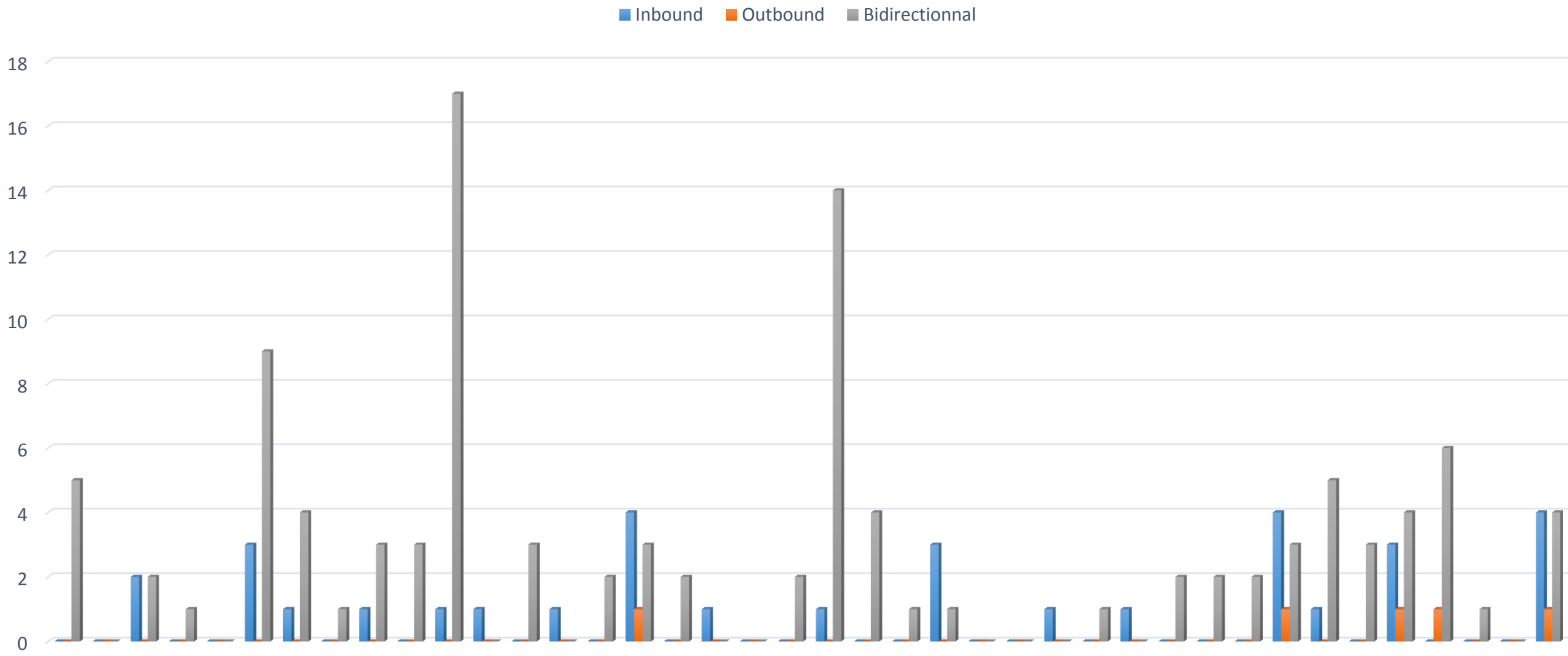
Top20 mots de passe sur 120K utilisateurs



COGICEO

Expertise technique en sécurité informatique

Trust domains outside the forest

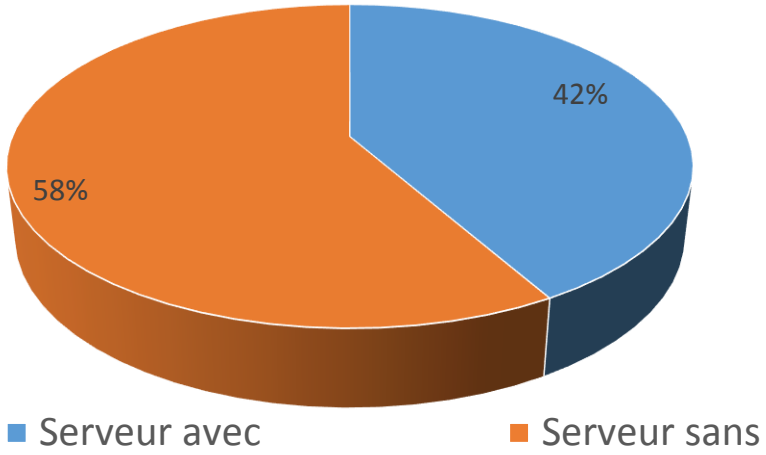


COGICEO

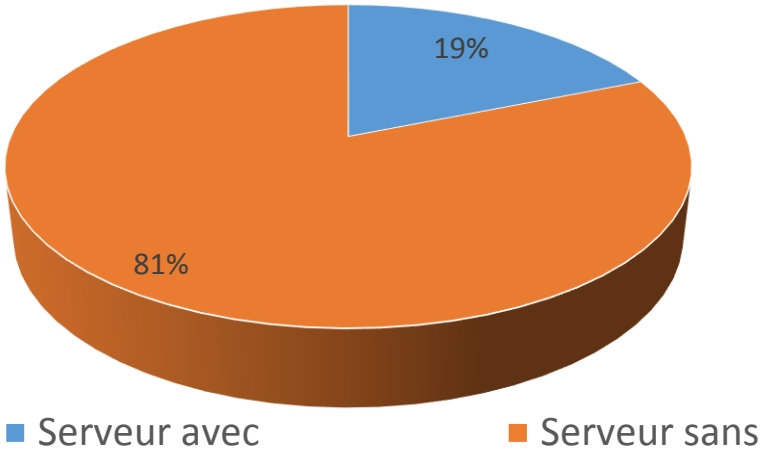
Expertise technique en sécurité informatique

Focus sur le domaine de 985 serveurs

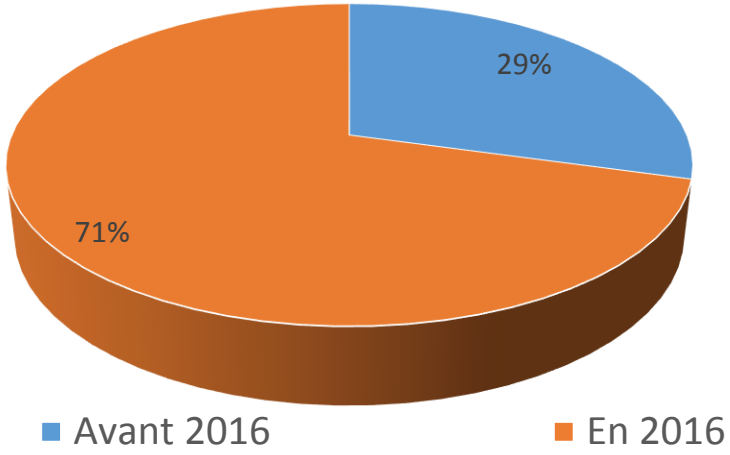
Tache planifiée possédant un compte admin sur 1 autre serveur



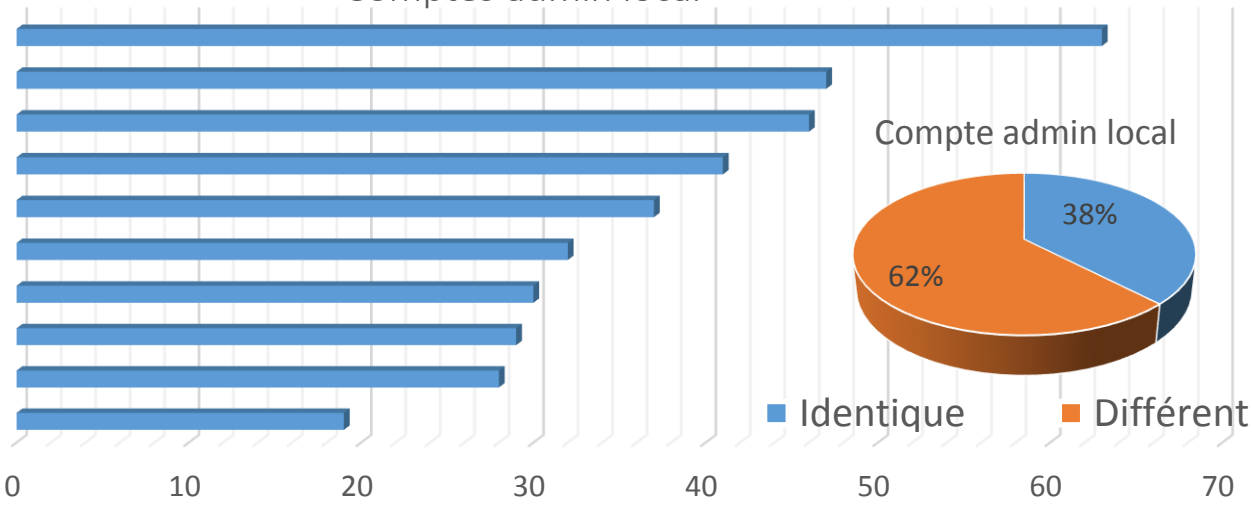
Service possédant un compte admin sur 1 autre serveur



Dernière mise à jour de sécurité



Comptes admin local



Cogiceo

Expertise technique en sécurité informatique

Sommaire

But

- Récupération automatique des données de sécurité
- Normalisation et centralisation dans une base de données
- Création automatique des liens entre les objets
- Analyse automatique des chemins de compromissions classiques
- Visualisation concise des résultats via des critères pertinents

COGICEO

Expertise technique en sécurité informatique

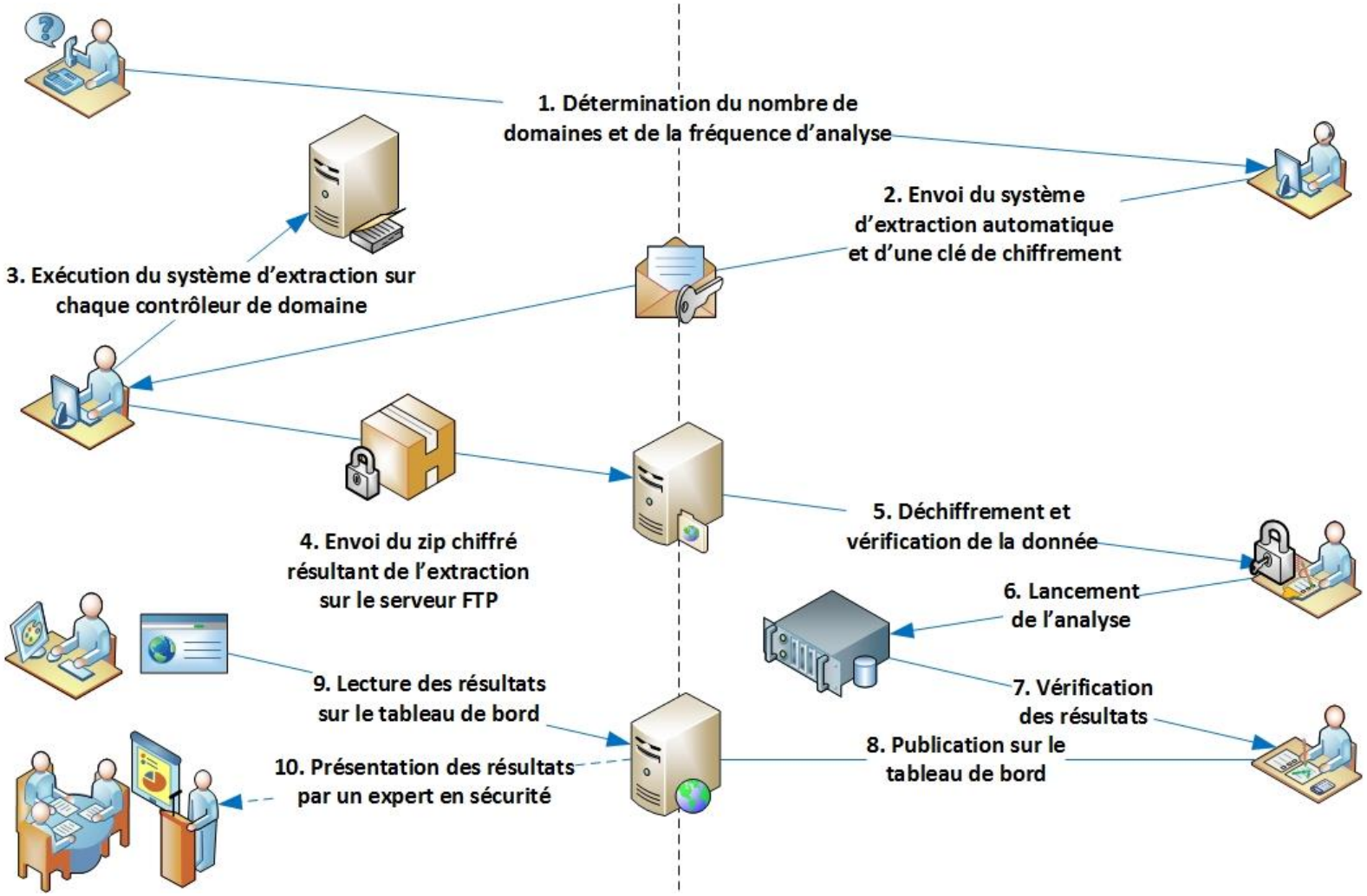
Avantages

- Extraction de la donnée séparée du traitement
- Extraction non intrusive avec peu de consommation de ressources
- Technique universelle rendant la collecte indépendante des niveaux du système d'exploitation
- Extraction n'impliquant ni installation d'outils ni ouvertures de flux autres que ceux utilisés par défaut
- Chiffrement des données assurant une confidentialité totale
- Vérification automatique de l'intégrité des données

COGICEO

Expertise technique en sécurité informatique

Cinématique



Expertise technique en sécurité informatique

Sommaire

COGICEO

Expertise technique en sécurité informatique

Bonnes pratiques

- Abandon des protocoles obsolètes
- Correctif de sécurité / Migration
- Fine grained password policy
- Bastion d'administration
- Cloisonnement réseau
- Séparation des rôles et des privilèges (administrateurs et serveurs)
- Microsoft Local Admin Password Solution
- Microsoft Managed service accounts
- Security Operating Center
- Audits récurrents
- Formation sécurité Microsoft


COGICEO
Expertise technique
en sécurité informatique
www.cogiceo.com
+33 (0)1.85.08.10.70
contact@cogiceo.com
www.twitter.com
/cogiceo
www.linkedin.com
/company/cogiceo