GEFONA
DIGITAL FOUNDATION

2020

ETATS DE LA SECURITE DES APPLICATIONS EN ENTREPRISES

Contacts:
@ hello@gefona.org
www.gefona.org
Yaoundé, Cameroun

CONTENU

I. INTRODUCTION

II. PRINCIPALES OBSERVATIONS

II.1 PORTEFEUILLE D'APPLICATIONS ET INFRASTRUCTURE NUMÉRIQUE

II.2 SURFACE DE LA MENACE ET TENDANCE DES ATTAQUES

II.3 ÉTAT DE PRÉPARATION DES ORGANISATIONS EN MATIÈRE DE SÉCURITÉ

II.4 RÉGLEMENTATION DE LA GARANTIE D'APPLICATION

III. CONCLUSION

ANNEXE I: MÉTHODOLOGIE DE RECHERCHE ET ÉCHANTILLONNAGE

ANNEXE II: RÉFÉRENCES

I. Introduction

Bienvenue à la première édition de l'État de la sécurité des applications dans les entreprises* (ESA) au Cameroun. Dans son document 2010/2020 intitulé Document de stratégie pour la croissance et l'emploi (DSCE) , le gouvernement camerounais s'est engagé à stimuler l'économie et le développement du pays par le biais des TIC. En effet, l'utilisation des TIC et l'industrie des TIC elle-même ont connu une croissance significative, le Cameroun étant en passe de devenir une plaque tournante des TIC en Afrique centrale [1]. Malheureusement, à mesure que la société se numérise, les cybermenaces se multiplient.

Mc Afee rapporte que la cybercriminalité coûte aux pays d'Afrique subsaharienne près de 1 654 milliards de francs CFA, soit 3 milliards de dollars [2] chaque année. Outre les pertes financières qu'elle entraîne, elle affecte aussi bien les particuliers que les entreprises et les organismes gouvernementaux, et elle dégrade la réputation, la marque et l'image. Ces attaques informatiques comprennent les escroqueries sentimentales, le chantage vidéo, les faux visas, les fausses offres d'emploi et de bourses, les cyber-arnaques et, plus récemment, les logiciels de rançon. Localement au Cameroun, de 2015 à 2017, l'ANTIC a identifié les attaques suivantes [3] :

- **Fraude à la carte de crédit : 3,7 milliards de francs CFA**
- **Fraude à la carte SIM : Plusieurs milliards de francs CFA**
- **L'escroquerie : 4 milliards de francs CFA**
- **Vol d'identité : Plusieurs centaines (182 fonctionnaires du gouvernement)**
- **Défaillances de sites web : 07 Sites web gouvernementaux**
- **Malwares : ~23,61% des sites web du gouvernement sont touchés**

Par conséquent, alors que l'utilisation des TIC et le secteur continuent à se développer au Cameroun, les questions suivantes restent sans réponse :

- **À quoi ressemble la tendance à la menace et aux attaques au Cameroun?**
- **Quel est le niveau de préparation des organisations en matière de sécurité?**
- **A quoi ressemble la réglementation de la sécurité des applications?**

Dans ce rapport où nous avons interrogé 42 entreprises au Cameroun et obtenu 137 réponses, à travers les secteurs privé et public, nous présentons à la fois l'environnement et l'état le plus actuel du contexte social et sécuritaire qui prévaut au Cameroun dans l'espace de la cyber sécurité. Dans ce numéro, vous trouverez une mise à joursur les menaces aux applications, une discussion sur les menaces émergentes, un aperçu de la part de marché des différents fournisseurs de sécurité, les normes les plus utilisées et quelques recommandations basées sur notre observation et les tendances de sécurité sur la façon dont les organisations au Cameroun peuvent mieux protéger leurs actifs contre les risques et les menaces. Y compris la manière dont les systèmes et les applications utilisés par le gouvernement peuvent être sécurisés, sécurisant ainsi le cyberespace camerounais et ses utilisateurs.

Par entreprise, nous entendons les organisations du secteur privé ou public comptant plus de 100 employés.

II. Principales conclusions

01

66,7% des applications utilisées dans les entreprises sont des applications traditionnelles de type client-serveur monolithique pour les ordinateurs de bureau.

03

16% des entreprises disposent d'un pare-feu d'application Web, dont seulement 8,4% effectuent des tests de pénétration.

02

56,3% de la menace qui pèse sur les applications et les données des entreprises est due à des attaques d'applications Web telles que SQLi, XSS, XXE et RCE et à une authentification frauduleuse entraînant une fraude.

04

39,2% des entreprises ont déclaré utiliser les normes locales de l'Agence nationale pour les technologies de l'information et de la communication (ANTIC) et un pourcentage égal d'entreprises utilisent la norme ISO27001.

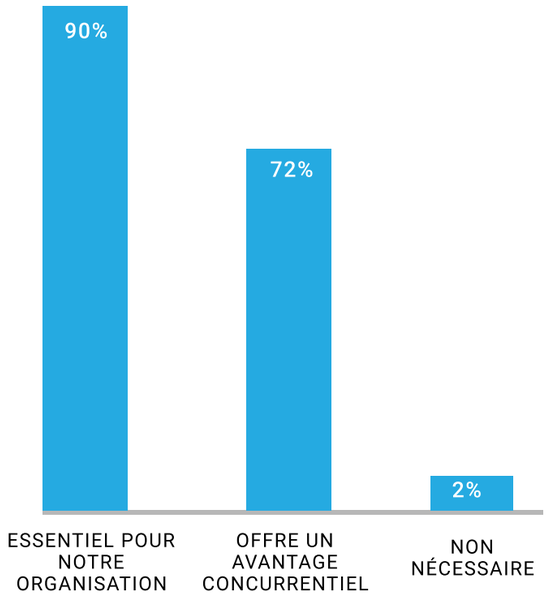
Portefeuille d'applications et infrastructure numérique

66,7% des applications utilisées dans les entreprises sont des applications traditionnelles de type client-serveur monolithique pour les ordinateurs de bureau.

La majorité des entreprises ont commencé leur parcours de développement mais admettent qu'il y a des défis à relever et sont conscientes du long chemin à parcourir. Le taux d'adoption des applications mobiles dans les entreprises est également en hausse et représente actuellement 17,5 % du portefeuille total d'applications.

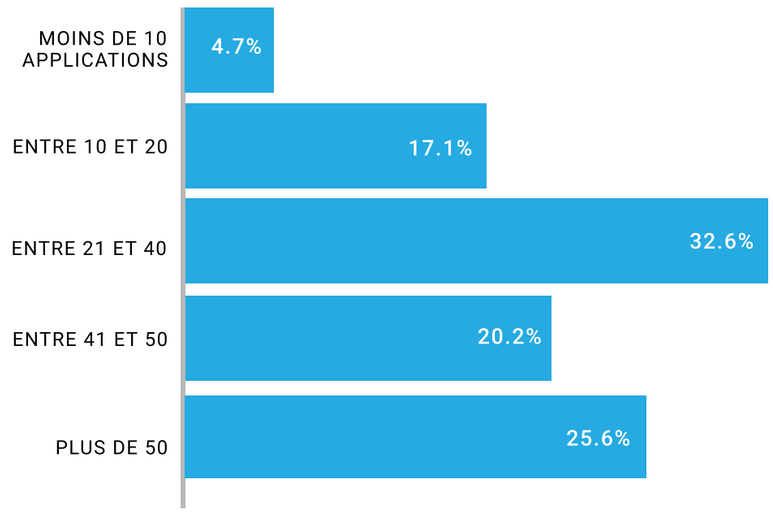
Nous avons demandé:

Quelle importance est donnée aux applications dans votre Organisation ?



Nous avons demandé:

Quelle est la taille de votre portefeuille d'applications (développées en interne ou commerciales) (par exemple : outlook, sagesaari, MS Excell, application de gestion...) ?



Nous avons appris que:

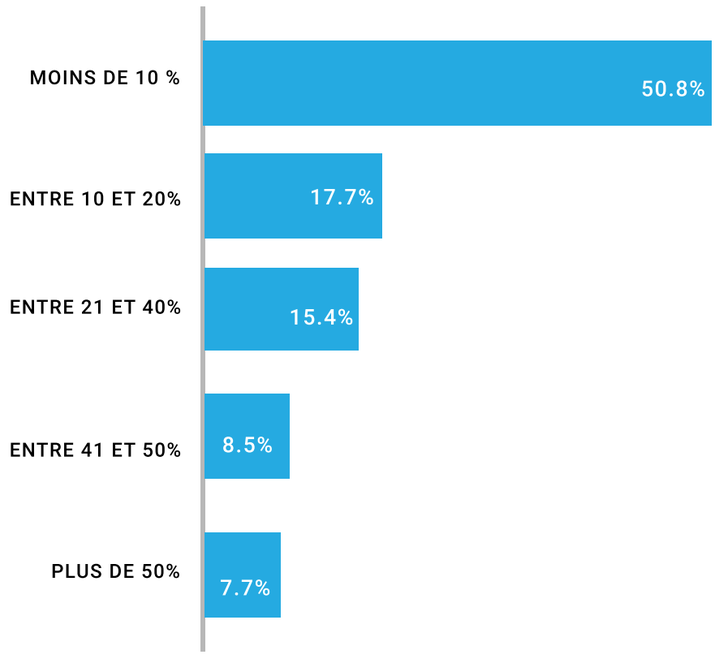
Une proportion importante des entreprises ont entre 21 et 40 applications dans leur portefeuille

Nous avons appris que:

En général, les entreprises sont plus nombreuses à externaliser le développement de leurs applications.

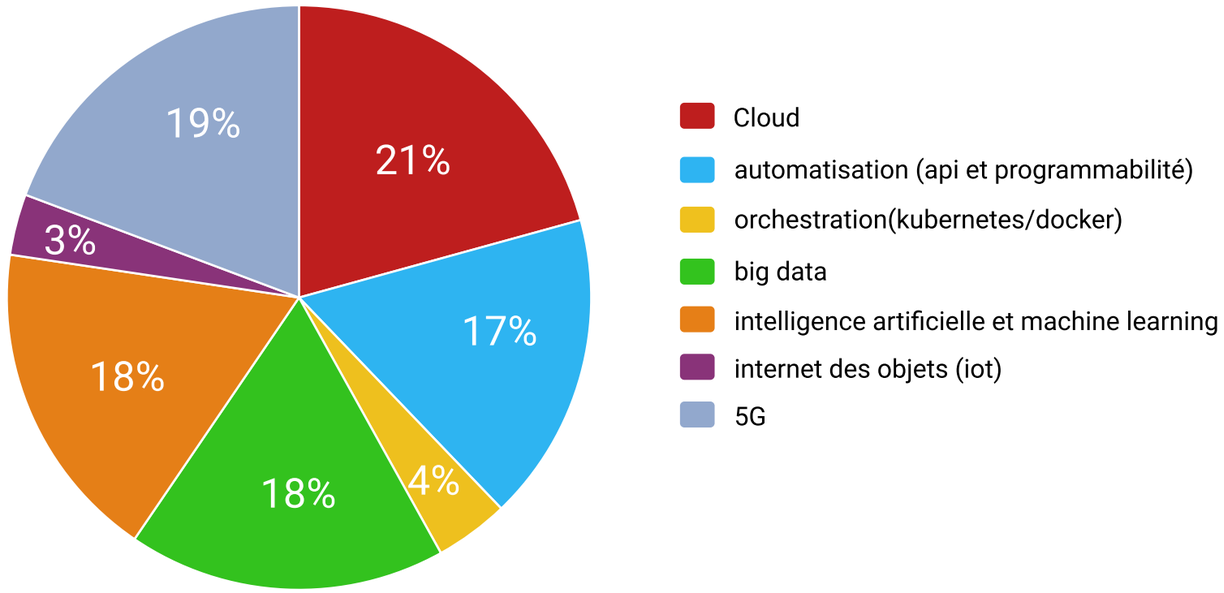
Nous avons demandé:

Quel est le pourcentage d'applications développées en interne ?



Nous avons demandé:

Selon vous, quelles tendances technologiques seront stratégiquement importantes pour vous au cours des deux à cinq prochaines années ?



Nous avons appris que:

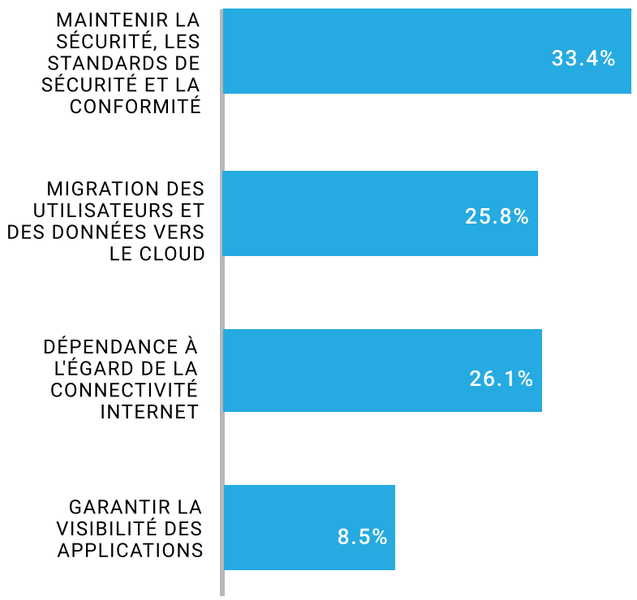
En général, les entreprises sont plus nombreuses à externaliser le développement de leurs applications.

Nous avons appris que:

Le cloud computing est actuellement a tendance technologique la plus importante sur le plan stratégique, bien que l'IA, les Big Data et l'automatisation soient également considérés comme stratégiquement importants par les entreprises camerounaises.

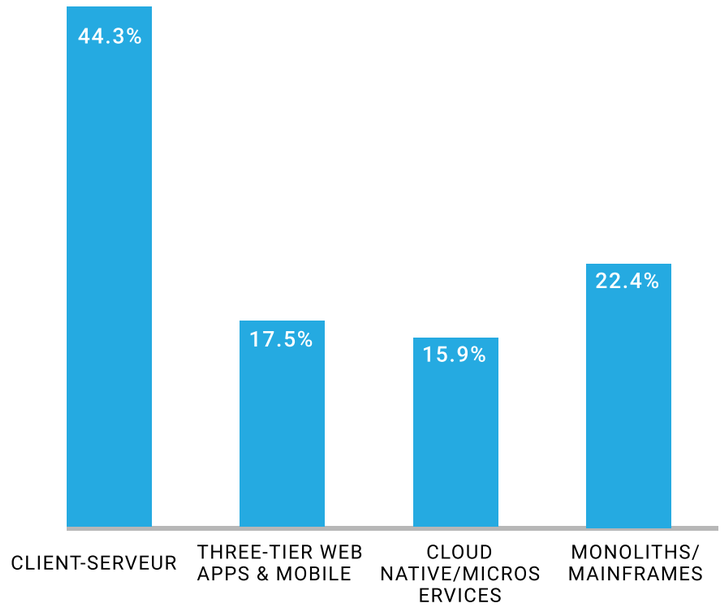
Nous avons demandé:

Lorsque vous pensez à la migration des applications vers le cloud, quels sont les aspects de la gestion de l'application que vous trouvez les plus frustrants ou les plus difficiles ?



Nous avons demandé:

Quelle est la carte actuelle de déploiement des applications dans votre organisation ?



Nous avons appris que:

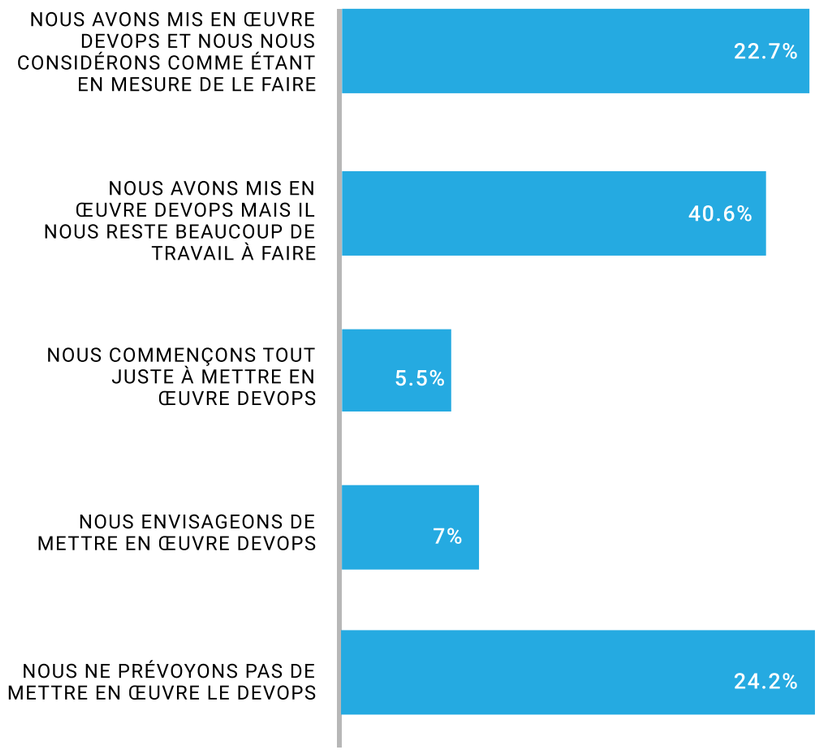
Le maintien de la sécurité, de la politique et de la conformité est le plus grand défi pour les entreprises camerounaises lors de la migration de leurs applications vers le cloud.

Nous avons appris que:

Les architectures d'applications client-serveur sont les plus courantes au Cameroun.

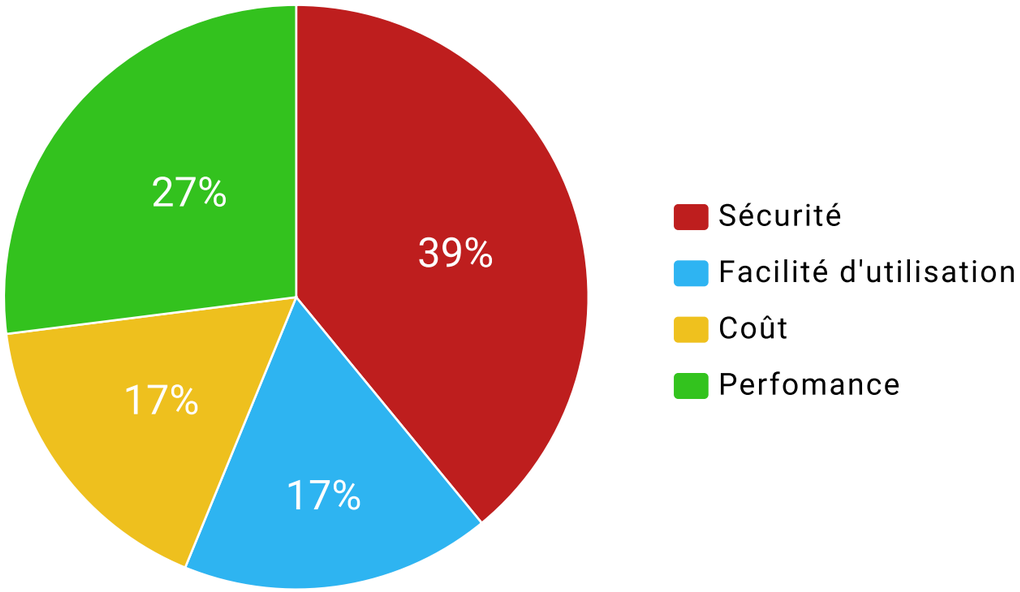
Nous avons demandé:

Où en est votre organisation dans son parcours vers le DevOps ?



Nous avons demandé:

Lorsque vous déployez une application, veuillez sélectionner votre première et votre deuxième préoccupation principale.



Nous avons appris que:

La plupart des organisations n'en sont qu'au tout début de leur parcours dans le cadre de DevOps

Nous avons appris que:

La plupart des organisations s'inquiètent surtout de la sécurité d'une application pendant son déploiement.

Un nombre important de répondants s'inquiètent également de la performance de la demande.

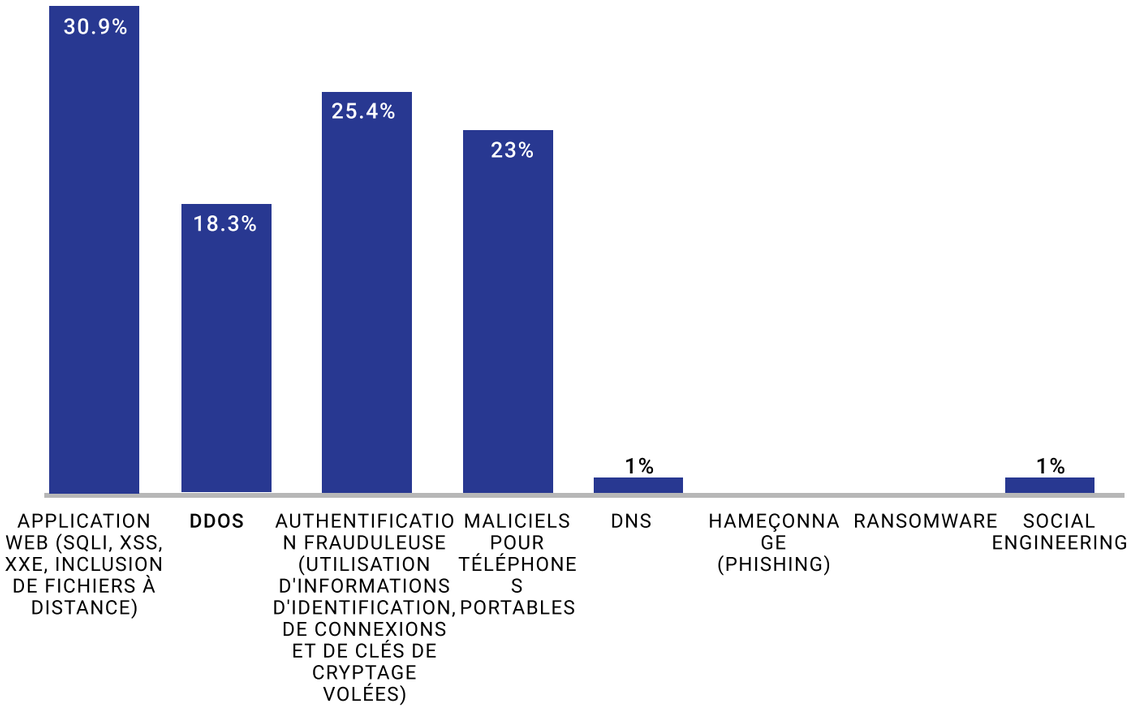
Surface de la menace et tendance des attaques

56,3% de la menace qui pèse sur les applications et les données des entreprises est due à des attaques d'applications Web telles que SQLi, XSS, XXE et RCE et à une authentification frauduleuse entraînant une fraude.

La grande majorité des répondants craignent surtout la perte ou la fuite de données à la suite d'un exploit. En outre, la sécurité est de plus en plus préoccupante, puisque 66,6 % des personnes interrogées déclarent avoir remarqué une augmentation des menaces au cours des 12 derniers mois.

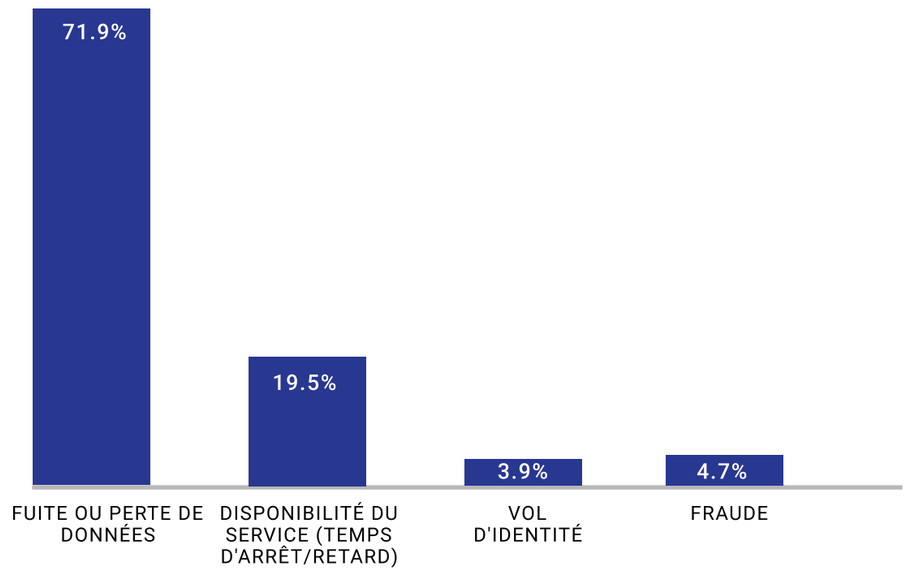
Nous avons demandé:

Comment les attaques externes sont-elles menées contre votre application ?



Nous avons demandé:

De quoi avez-vous le plus peur?



Nous avons appris que:

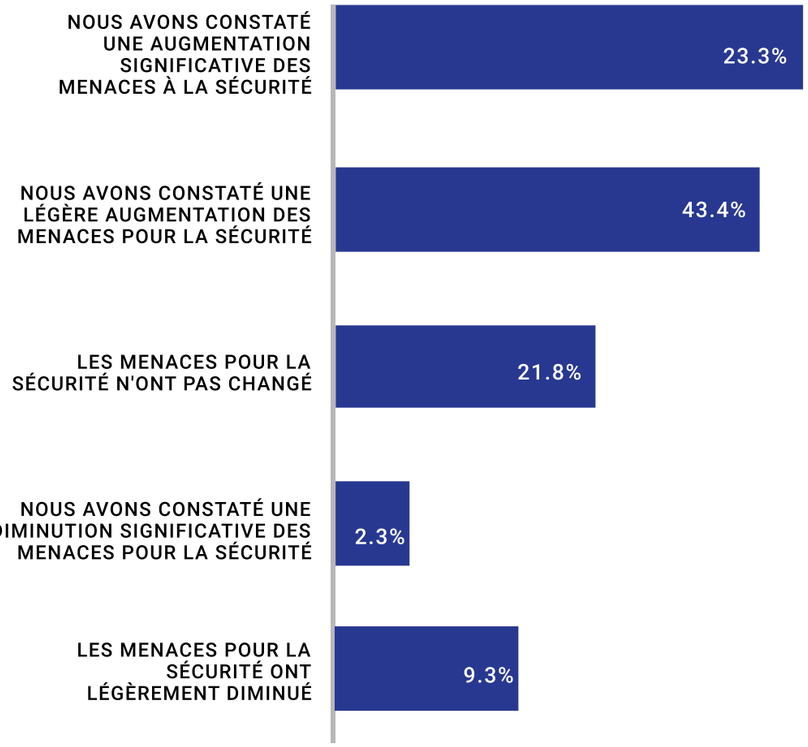
La plupart des attaques externes se sont par le biais d'applications web

Nous avons appris que:

Les entreprises camerounaises craignent surtout une fuite ou une perte de données.

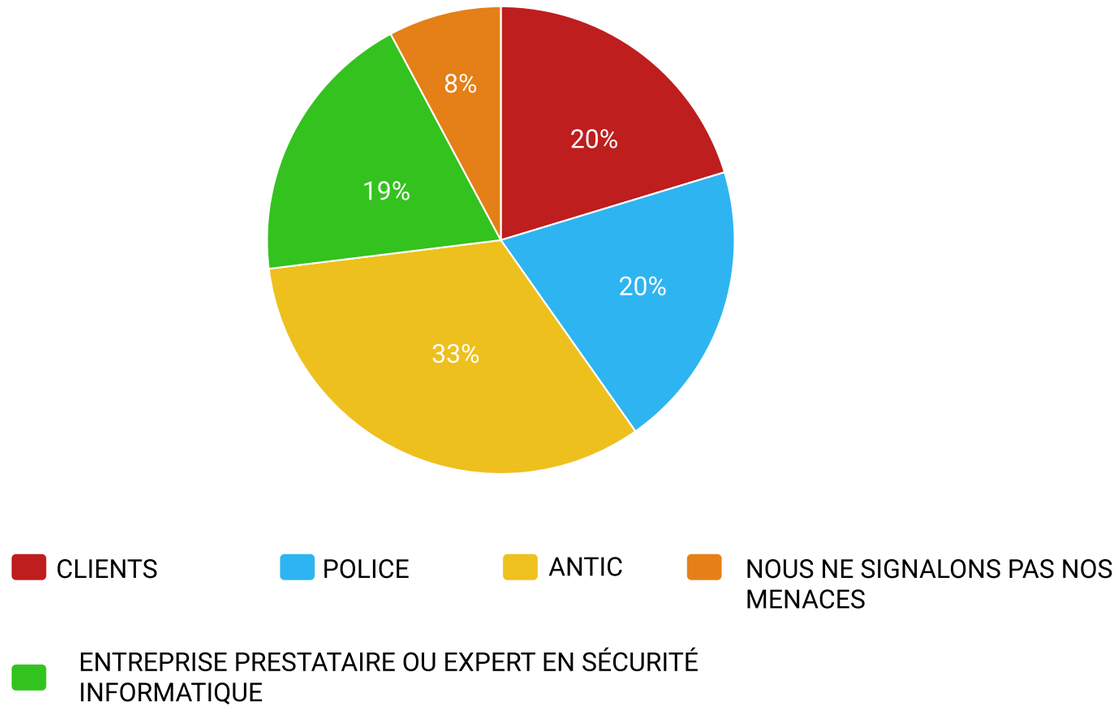
Nous avons demandé:

Votre organisation a-t-elle constaté une différence dans le nombre de menaces pour la sécurité au cours des 12 derniers mois ?



Nous avons demandé:

A qui / quelle organism votre organisation signale t'elle les menaces auxquelles elle fait face ?



Nous avons appris que:

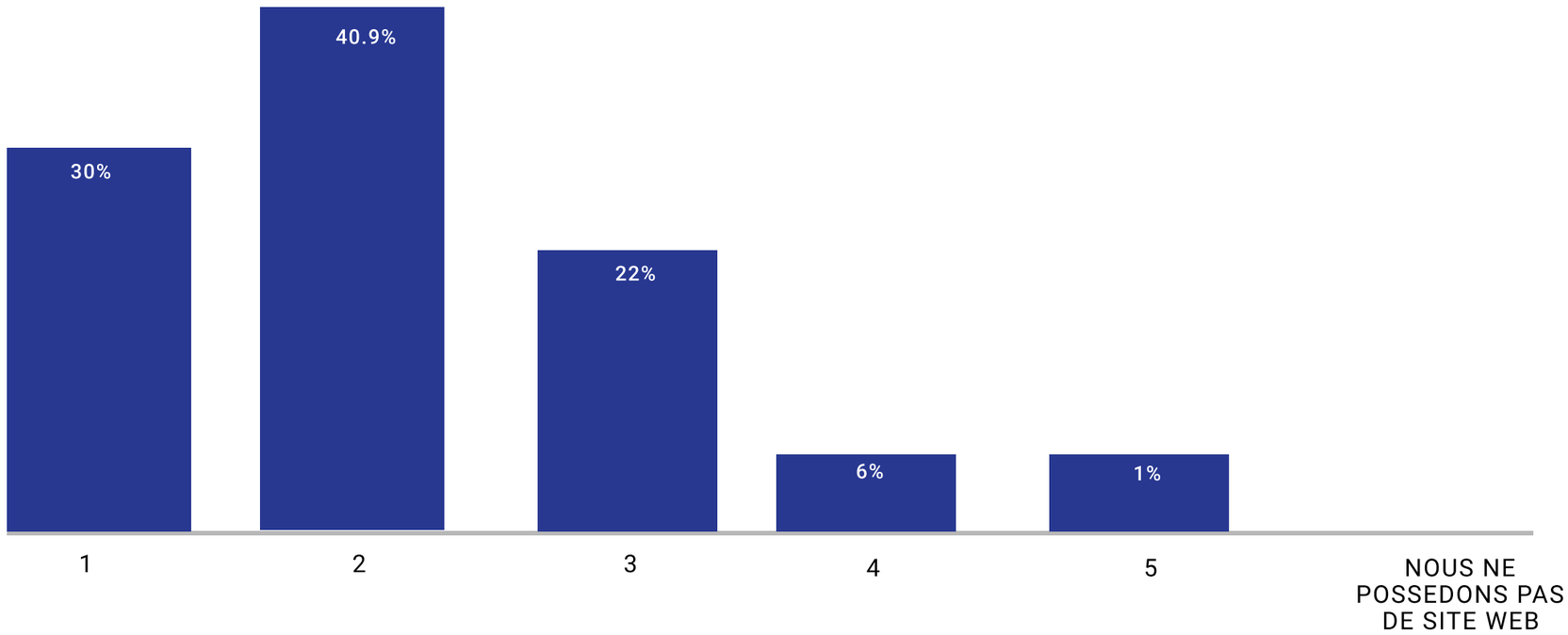
Quelques organisations ont vu leurs menaces de sécurité augmenter de manière significative au cours des 12 derniers mois, mais en général, il n'y a eu qu'une légère augmentation des attaques de sécurité contre les entreprises au Cameroun au cours des 12 derniers mois.

Nous avons appris que:

Les entreprises camerounaises notifient les parties prenantes d'une faille de sécurité, mais elles en informent principalement l'organisme de régulation ANTIC et seules quelques-unes en informent les clients.

Nous avons demandé:

Quel est le degré de vulnérabilité du site web de votre organisation ?



Nous avons appris que:

La plupart des entreprises considèrent que la vulnérabilité de leur site web est moyenne.

État de préparation des organisations en matière de sécurité

16% des entreprises disposent d'un pare-feu d'application Web, dont seulement 8,4% effectuent des tests de pénétration.

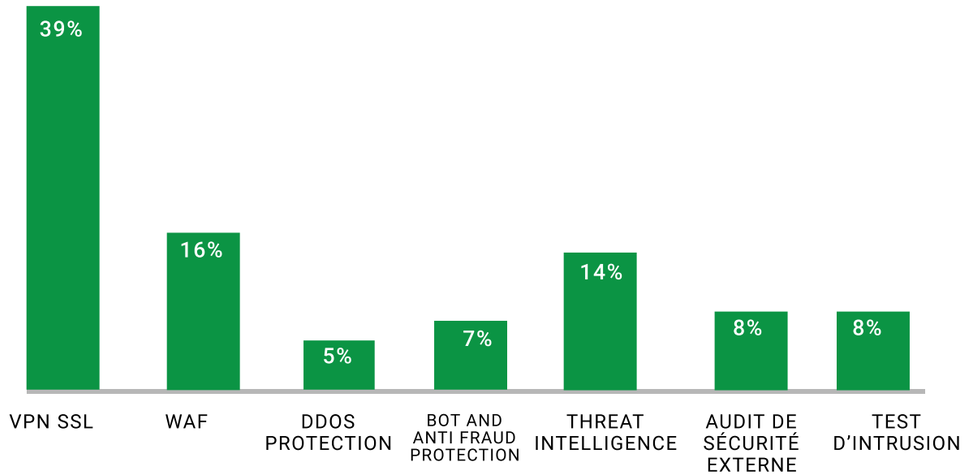
Cela montre que la majorité des entreprises se concentrent encore sur la sécurité au niveau du réseau et que les entreprises camerounaises ont encore beaucoup à faire en matière de sécuritédes applications.

71% pensent que la sécurisation des informations des clients est la plus importante en ce qui concerne la sécurité des applications, ce qui signifie que la protection des données des clients est une priorité pour la plupart des entreprises.

Alors qu'une faille de sécurité accélérerait le processus d'achat de sécurité pour la plupart des entreprises, plus de 85 % ont déclaré utiliser des solutions de sécurité des applications et des testeurs internes.

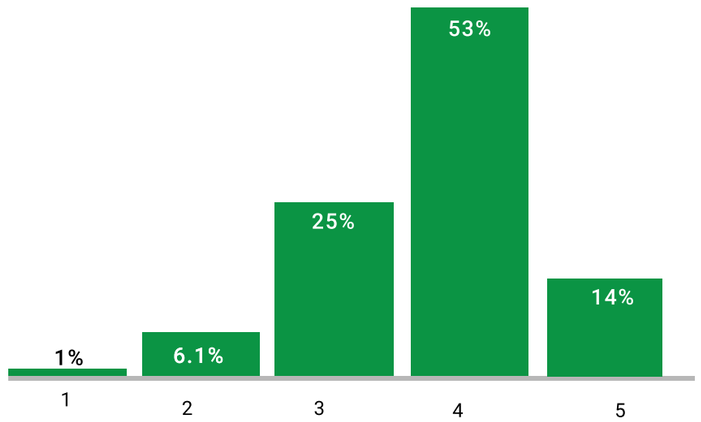
Nous avons demandé:

Parmi les services de sécurité suivants, lequel votre organisation déploie-t-il actuellement ?



Nous avons demandé:

Sur une échelle de 1 à 5 (1 étant le plus faible et 5 le plus élevé), quel est votre degré de confiance dans la capacité de votre entreprise à résister à une attaque contre vos demandes ?



Nous avons appris que:

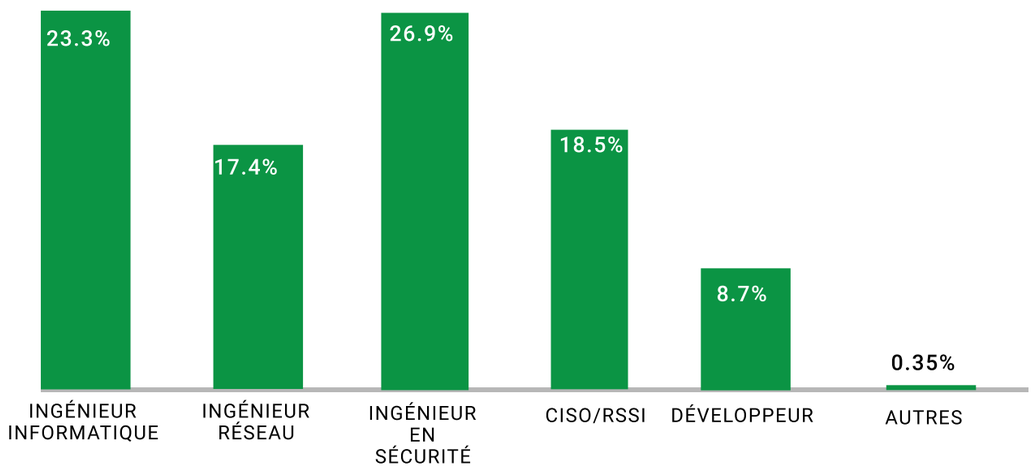
Au Cameroun, les entreprises se concentrent sur la sécurité au niveau du réseau, comme les VPN SSL

Nous avons appris que:

Les entreprises sont convaincues de leur capacité à résister à une attaque contre leurs applications.

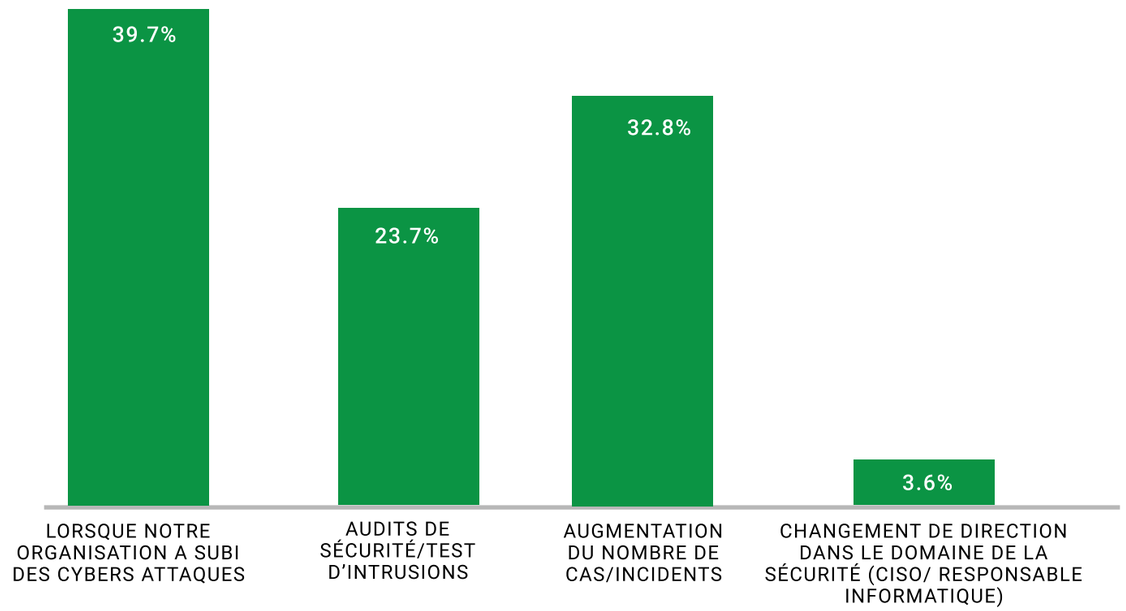
Nous avons demandé:

Quels sont les rôles au sein de votre organisation qui sont principalement responsables de la sécurisation de vos applications ?



Nous avons demandé:

Quels sont les événements qui "accélèrent" le besoin et le processus d'achat de solutions de sécurité ?



Nous avons appris que:

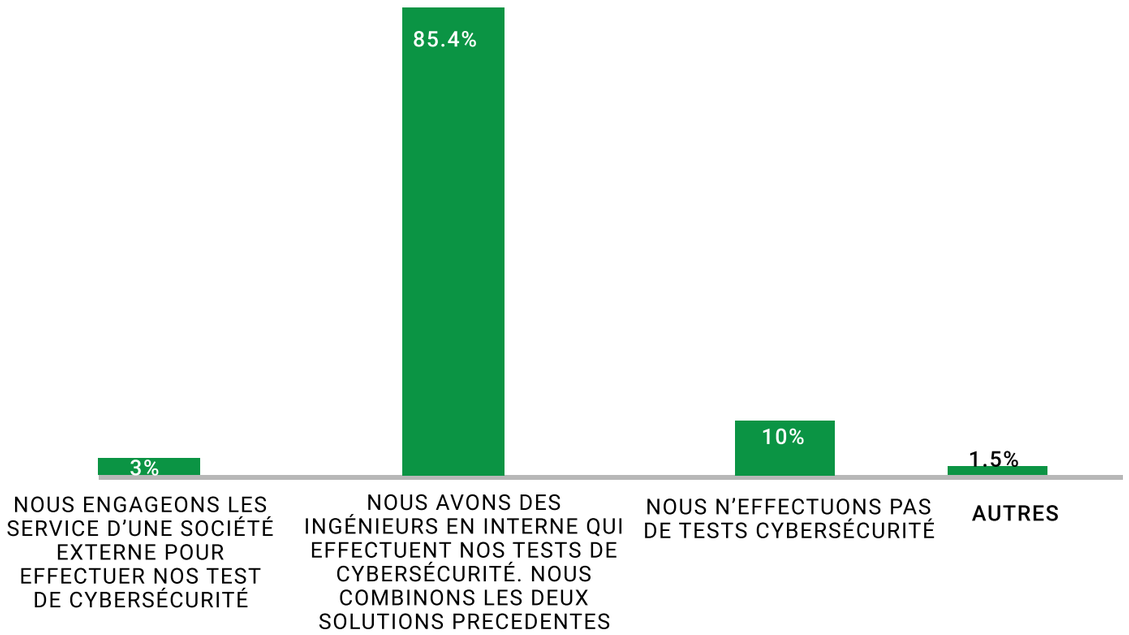
La plupart des entreprises n'engagent pas d'ingénieur en sécurité pour sécuriser leurs systèmes. Elles laissent leur équipe informatique habituelle faire le travail de sécurité.

Nous avons appris que:

Les entreprises admettent une faille de sécurité ou une augmentation du nombre d'incidents plutôt qu'un changement de direction du département informatique, ce qui accélérera les décisions en matière de dépenses de sécurité.

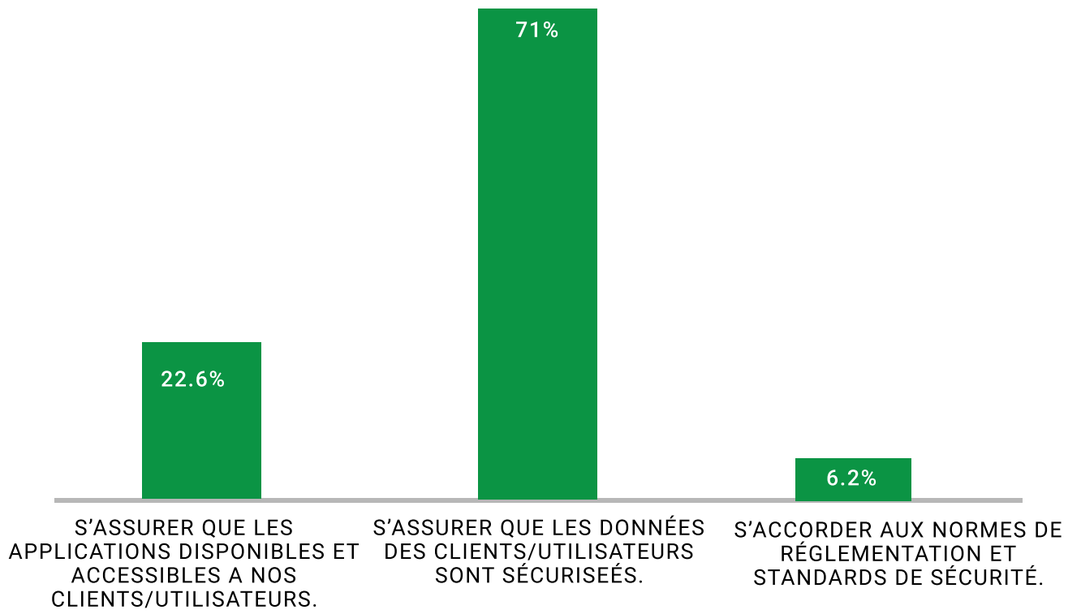
Nous avons demandé:

Comment votre organisation gère-t-elle actuellement les tests de sécurité des applications ?



Nous avons demandé:

Que considérez-vous comme le plus important en matière de sécurité des demandes ?



Nous avons appris que:

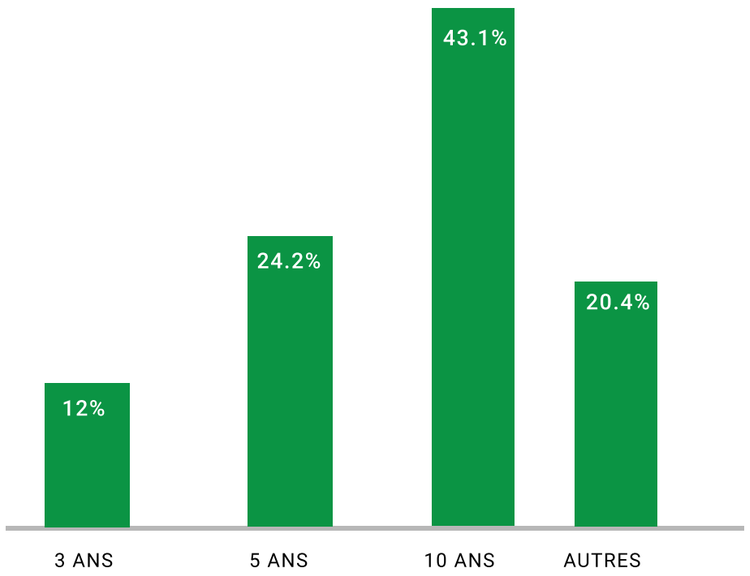
L'équipe informatique interne effectue des tests de sécurité des applications pour la majorité des entreprises.

Nous avons appris que:

Garantir la sécurité des données des clients est ce que les entreprises camerounaises considèrent comme le plus important en matière de sécurité des applications.

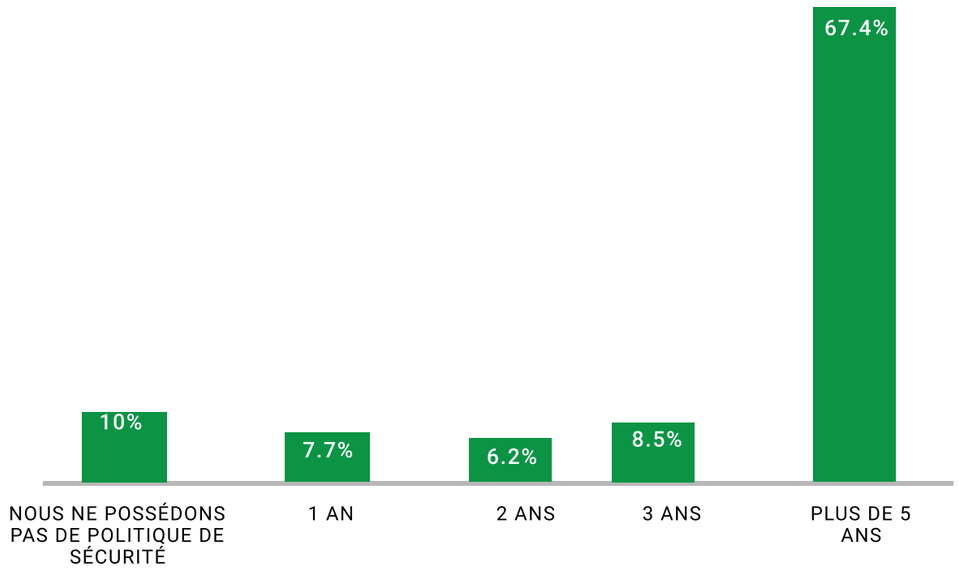
Nous avons demandé:

Pendant Combien de temps conservez-vous les données opérationnelles et de trafic dans votre organisation ?



Nous avons demandé:

Depuis combien de temps avez-vous une politique de cybersécurité ?



Nous avons appris que:

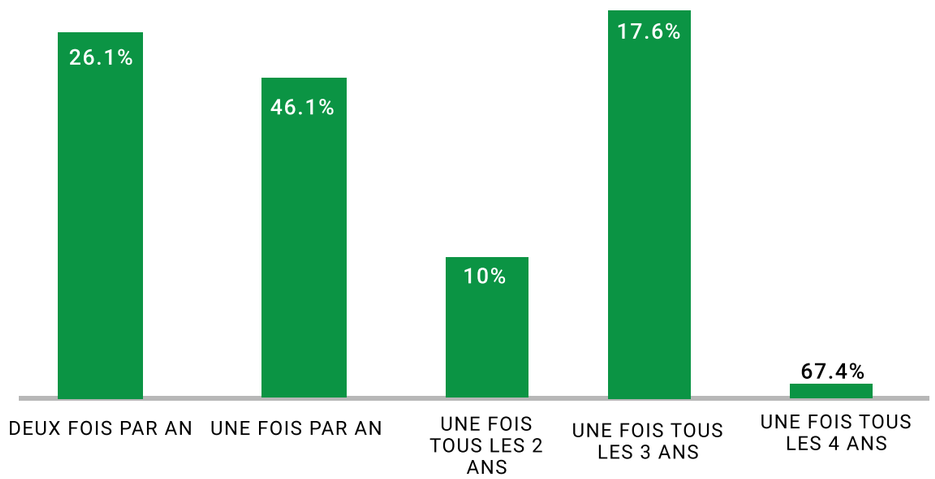
Il est courant de conserver les données opérationnelles jusqu'à 10 ans au Cameroun.

Nous avons appris que:

La plupart des entreprises ont une politique de cybersécurité depuis plus de 5 ans, tandis que quelques-unes n'en ont pas.

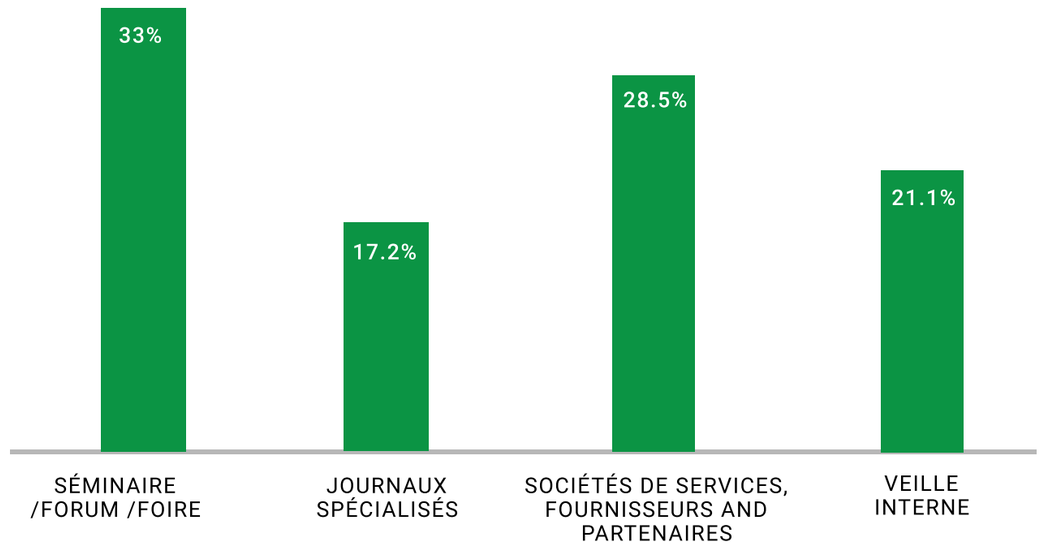
Nous avons demandé:

À quelle fréquence votre organisation procède-t-elle à des audits de cybersécurité ?



Nous avons demandé:

Comment votre organisation se tient-elle au courant des menaces et des solutions en matière de sécurité ?



Nous avons appris que:

La plupart des entreprises effectuent un audit de cybersécurité une fois par an.

Nous avons appris que:

Les séminaires et les sommets sont le principal moyen pour les entreprises camerounaises de se tenir au courant des menaces et des solutions en matière de sécurité.

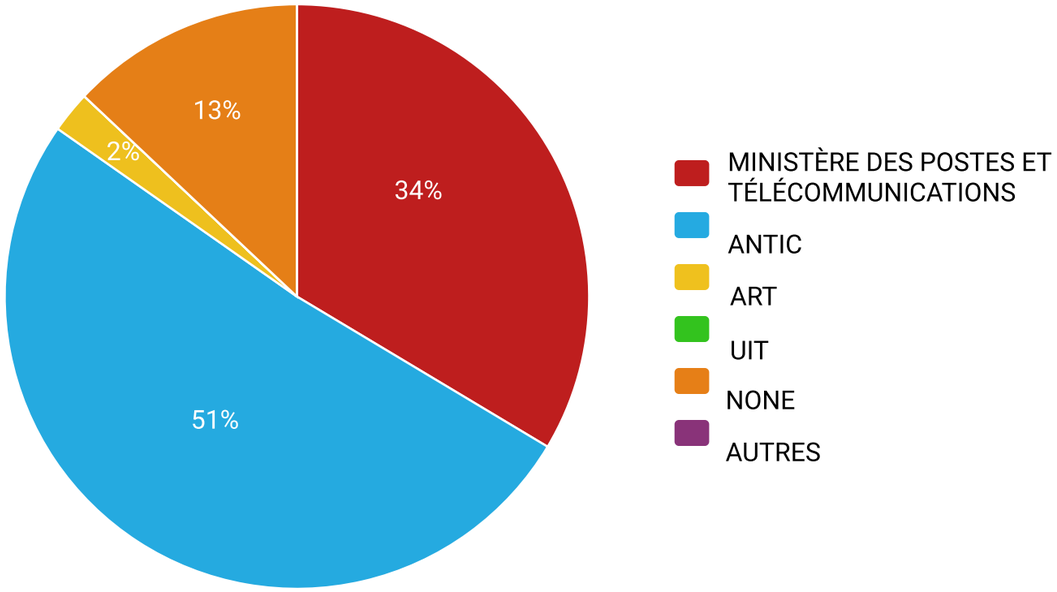
Réglementation de la sécurité des applications

39,2% des entreprises ont déclaré utiliser les normes locales de l'Agence nationale pour les technologies de l'information et de la communication (ANTIC) et un pourcentage égal d'entreprises utilisent la norme ISO27001.

Cela expliquerait pourquoi 51,1% des entreprises déclarent collaborer avec l'ANTIC plus que tout autre organisme de réglementation du pays.Seulement 3,6% des entreprises interrogées n'utilisent pas l'infrastructure PKI pour sécuriser leurs applications, ce qui est un bon signe en termes de sensibilisation à la sécurité dans le pays. Les certificats SSL signés par l'ANTIC sont aussi courants que les certificats signés par DIGICERT et SYMANTEC.40,3% des répondants ont déclaré utiliser le fournisseur de sécurité Cisco et 30,6% utiliser la solution Checkpoint

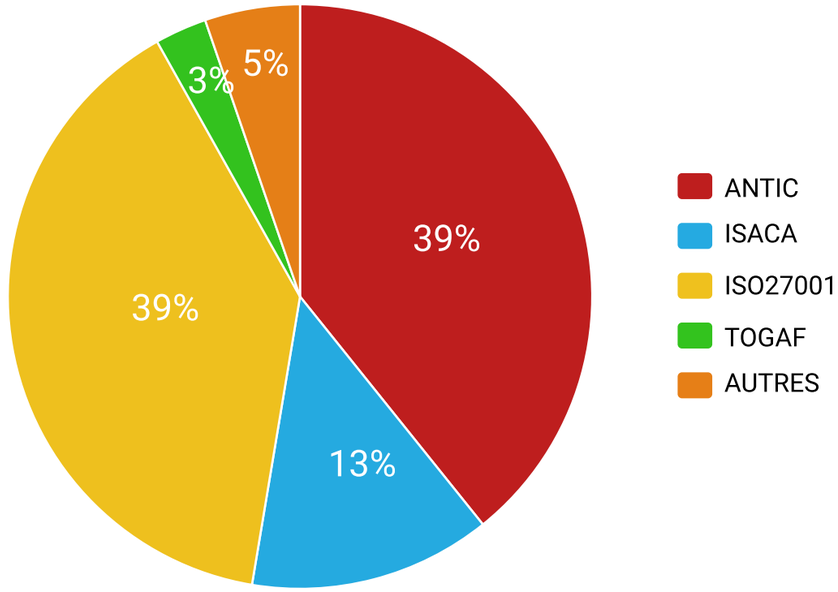
Nous avons demandé:

Parmi les institutions suivantes, avec laquelle votre organisation collabore-t-elle ?



Nous avons demandé:

Quels sont les règlements ou les normes appliqués par votre organisation ?



Nous avons appris que:

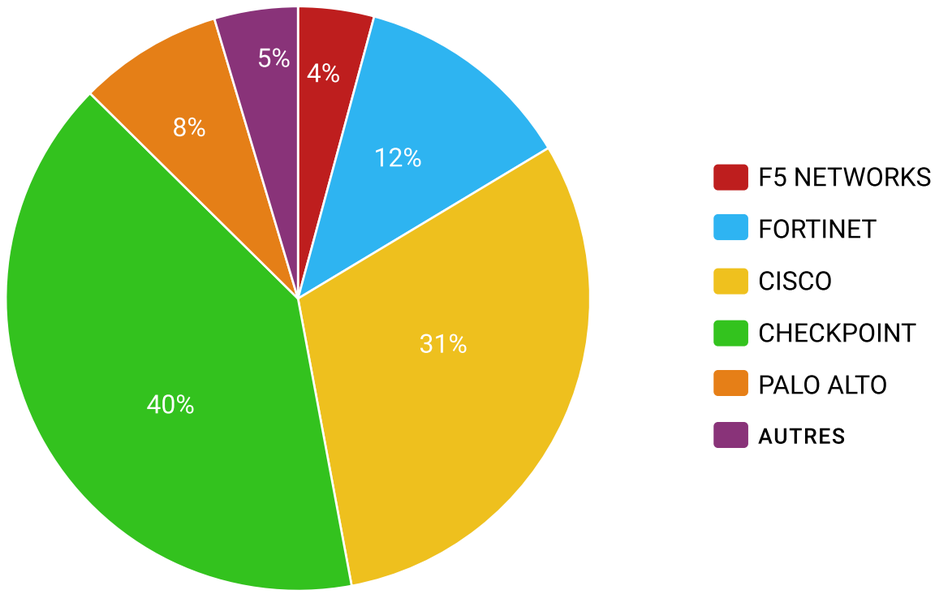
Les entreprises camerounaises collaborent principalement avec le régulateur local ANTIC

Nous avons appris que:

Les normes et la réglementation communément respectées au Cameroun sont l'ANTIC et l'ISO27001.

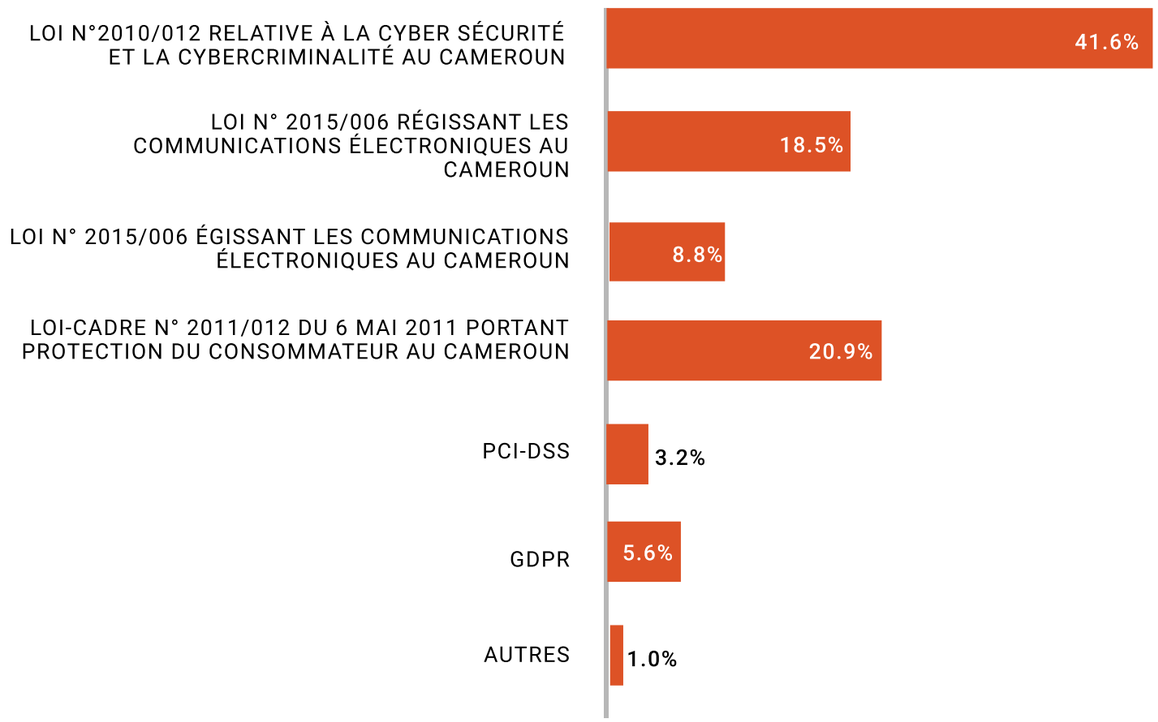
Nous avons demandé:

Quels sont vos équipements de solutions de sécurité informatique ?



Nous avons demandé:

parmis les regulations suivantes donnez celles que vous utilisez habituellement



Nous avons appris que:

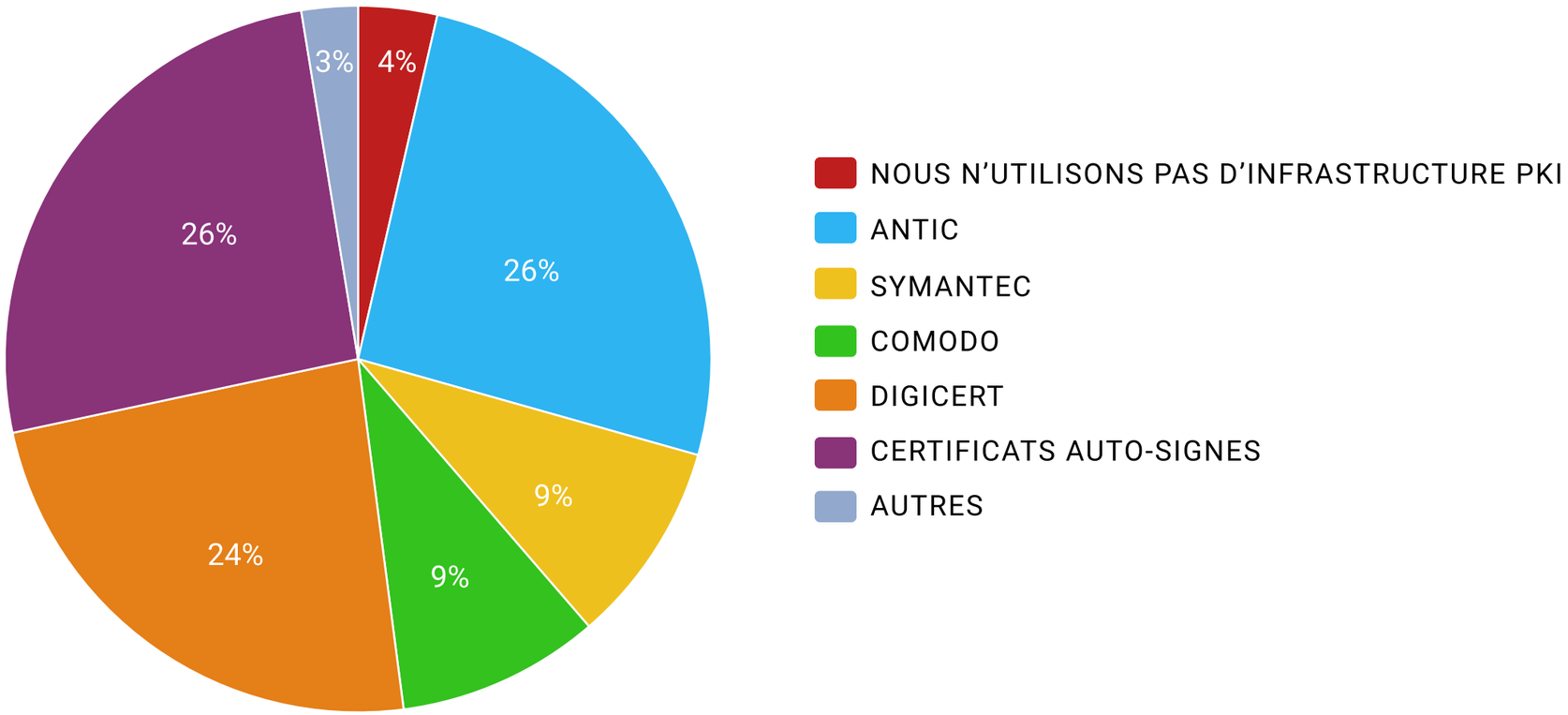
Cisco détient environ 40 % des parts du marché de la sécurité, suivi par Checkpoint avec environ 30,6 %.

Nous avons appris que:

Les entreprises cherchent à se conformer à la loi n° 2010/012 du 21 décembre 2010 sur la cybersécurité et la cybercriminalité au Cameroun plus que toute autre loi. Et seulement 5 % des entreprises environ se conforment au PIBR de l'UE.

Nous avons demandé:

Quelle autorité de certification utilisez-vous pour protéger vos données et vos applications ?



Nous avons appris que:

Les certificats signés ANTIC et Digicert sont couramment utilisés au Cameroun. Seul un très petit nombre d'entre eux n'utilisent pas l'ICP ou les certificats autosignés.

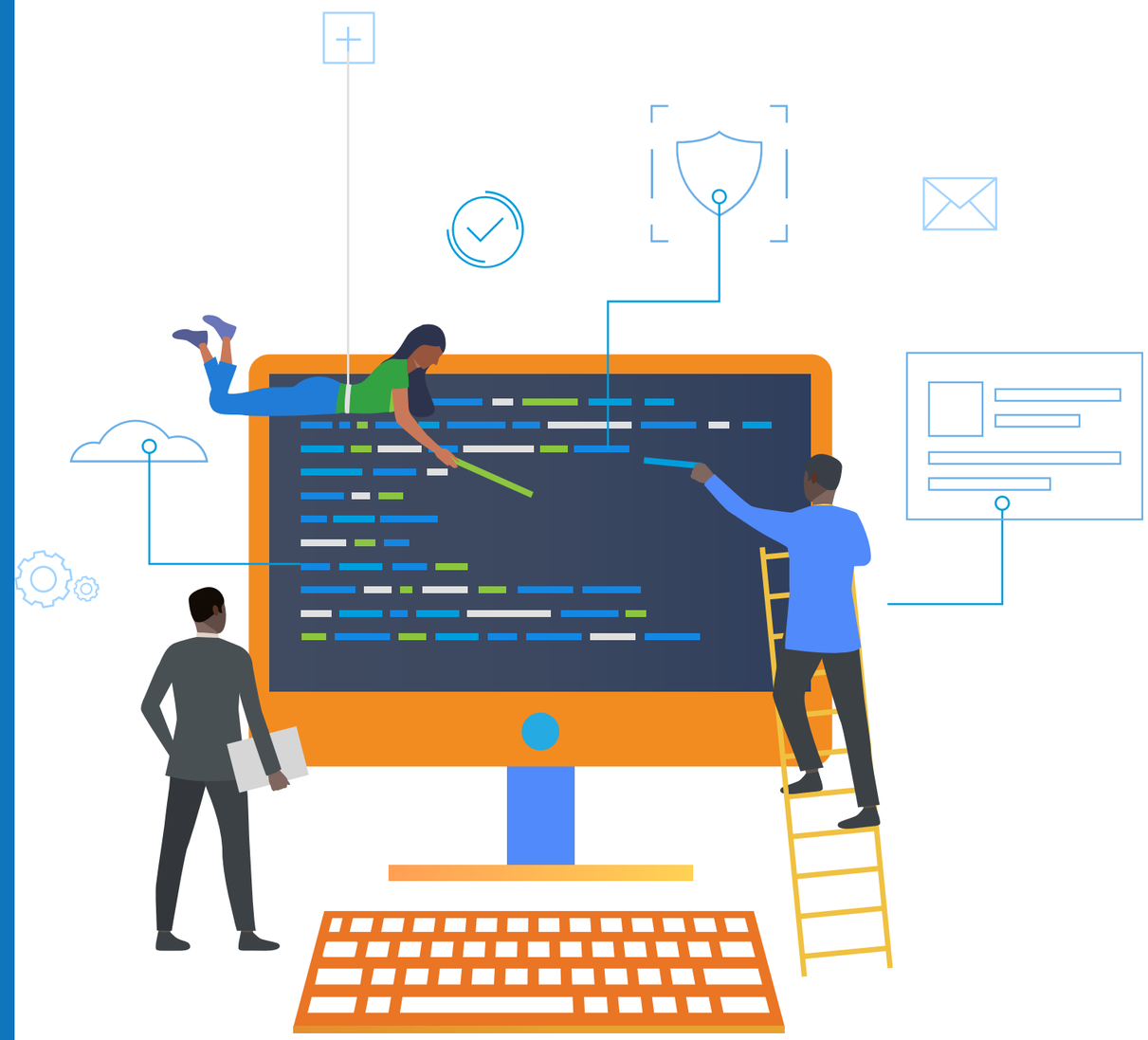
III. Conclusion

Dans cette étude, nous avons voulu répondre à trois questions principales :

- Comment se présente la menace au Cameroun et quelle en est la tendance ?
- Quel est l'état de préparation des organisations en matière de sécurité ?
- Et comment se présente la réglementation de la sécurité d'application au Cameroun ?

D'après les résultats de l'étude, il est clair que si les entreprises camerounaises sont conscientes des menaces de sécurité et des risques pour leurs systèmes en général, elles ne prêtent pas beaucoup d'attention à la sécurité au niveau des applications. L'étude montre que la plupart des entreprises semblent encore se concentrer sur la sécurité au niveau du réseau, laissant leurs applications vulnérables aux attaques de piratage et à l'exploitation. En conséquence, les dix premières attaques de l'OWASP et les authentifications non valides sont pertinentes, avec un énorme potentiel de fraude et de perte/fuite de données. Une raison possible à cela est le fait que la plupart des entreprises en sont aux premiers stades de leur parcours de DevOps et de la domination des architectures d'applications monolithiques dans les entreprises. Cela représente non seulement une opportunité de sensibilisation dans les organisations, mais aussi une opportunité de croissance des revenus pour le secteur de la cyber sécurité camerounais et les fournisseurs de sécurité.

En outre, l'étude a montré qu'en ce qui concerne la conformité aux normes et réglementations en matière de sécurité de l'information, la plupart des entreprises se concentrent sur la conformité aux normes et réglementations locales. Bien que cela soit prévisible, le très faible taux de conformité avec le règlement général européen sur la protection des données (RGDP) ou l'accent mis sur celui-ci pourrait indiquer une faible offre de services aux non-Africains et des relations d'affaires avec des consommateurs extérieurs au continent.



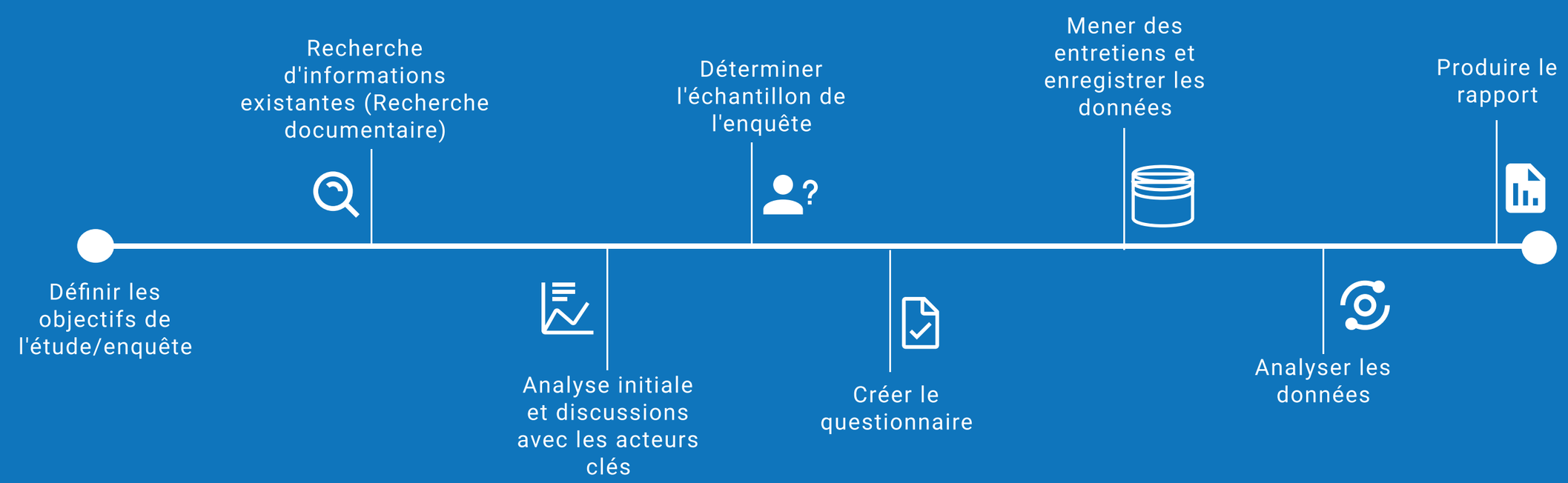
ANNEX I: Méthodologie de recherche et échantillonnage

Méthodologie de recherche

Cette étude a débuté par une recherche documentaire visant à comprendre l'écosystème de la sécurité numérique des entreprises au Cameroun tout en recueillant les informations disponibles et en identifiant les lacunes en matière d'information. Nous avons résumé les résultats de la recherche documentaire dans l'article **WEB SPACE: SOMMES NOUS EN SECURITE ?** publié sur www.gefona.org. Suite à l'étude documentaire, nous avons organisé des discussions formelles et informelles avec les acteurs clés du cyberespace camerounais afin d'affiner l'étude et de percevoir les premières tendances.

Nous avons ensuite conçu un questionnaire afin de faire le point sur l'état actuel de la sécuriténumérique, de confirmer les tendances initiales et de fournir les informations manquantes. Nous avons utilisé une combinaison d'entretiens en ligne (médias sociaux et courriels), par téléphone et en personne (face-à-face). À partir des informations recueillies lors de l'entretien,nous avons analysé les données et en avons tiré des enseignements.

En général, notre méthodologie de recherche est la suivante :



ANNEX II: REFERENCES

[1] Gouvernement du Cameroun. 2010/2020 Document de stratégie pour la croissance et l'emploi.

https://www.cameroonembassyusa.org/mainFolder/images/documents_folder/quick_links/Cameroon_DSCE_English_Version_Growth_and_Employment_Strategy_Paper_MONITORING.pdf

[2] McAfee (2018). Impact économique de la cybercriminalité - Pas de ralentissement. Consulté sur **https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html**

[3] Rapport sur la Cybercriminalité et la Cybersécurité au Cameroun de 2015 A 2017. ANTIC **https://www.antic.cm**

[4] Institut National de la Statistique. Répertoire démographique des entreprises modernes en 2016 4ème édition **http://www.statistics-cameroon.org/**

GEFONA
DIGITAL FOUNDATION

2020 GEFONA tous droits réservés