GEFONA
DIGITAL FOUNDATION

2020

STATE OF APPLICATION SECURITY IN ENTERPRISES

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

CONTENT

I. Introduction

Welcome to the First Edition of the State of Application Security in Enterprise* (ESA) in Cameroon. Cameroon's government committed to boost the economic and development of the country through the use of Information and Communication Technology (ICT) and indeed there has been significant growth both in the use of ICT and the ICT industry itself, with Cameroon moving towards becoming an ICT hub in central Africa [1]. Unfortunately, as the society becomes more digitized, so too do cyber threats grow.

McAfee reports that cybercrime costs sub-Saharan African countries nearly XAF1654 billion [2] every year. Beside financial losses on individuals as well as businesses and government agencies, reputation, brand and image are also affected. These computer attacks include dating/romance scams, video blackmail, fake visas, bogus job offers and scholarships and more recently ransomware attacks. Locally in Cameroon, from 2015 to 2017, ANTIC identified the following attacks [3]:

- **Credit card fraud: XAF3.7 billion**
- **SIMBOX fraud: Several XAF billion**
- **Scaming: XAF4 billion**
- **Identity theft: Several hundred (182 Governments Officials)**
- **Website defacements: 07 Government websites**
- **Malwares: ~23.61% of Government websites affected**

Therefore as ICT use and the sector continue to grow in Cameroon, the following questions remain unanswered:

- **How does the threat attack surface and trend in Cameroon look like?**
- **How are organizations' security readiness?**
- **How does regulation of application security look like?**

In this report where we surveyed 42 enterprises in Cameroon and got 137 responses, across private and public sectors, we present both the environment and the most current state of the social and security context that prevails in Cameroon in the cyber security space; In this issue you will find an update on threats to applications, a discussion of emerging threats, an overview of the market share of different security vendors, the most used standards and some recommendations based on our observation and security trends on how organizations in Cameroon can better protect their assets against risks and threats. Including how systems and applications used by the government can be secured, thereby securing Cameroon's cyberspace and its users.

* By entreprise, we refer to organizations in the private or public sector with 100+ employees.

II. Key Findings

01

66.7% of apps used in enterprises are traditional Monolithic Client-servers desktops apps.

02

56.3% of the Threat Surface to enterprise apps and data is due to Web application attacks such as SQLi, XSS, XXE, and RCE and to Broken authentication leading to Fraud.

03

16% of enterprises have a Web Application Firewall, with only 8.4% performing Penetration Testing.

04

39.2% of enterprises said they used the local National Agency for Information & Communication Technologies (ANTIC) standards and an equal percentage of enterprises use the ISO27001 standard.

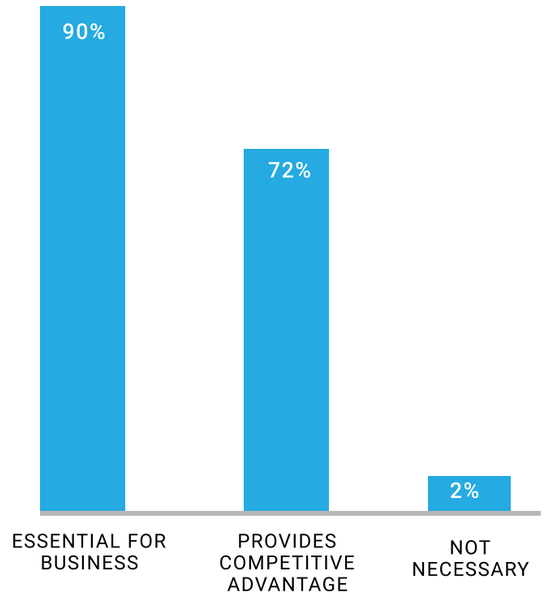
App portfolio and digital infrastructure

66.7% of apps used in Enterprises are traditional Monolithic Client-servers desktops apps.

The majority of enterprises have started their DevOps journey but admit challenges and are cognizant of the long road ahead. Mobile apps adoption rate in enterprises is also growing and currently at 17.5% of total app portfolio.

We asked:

How important is Application Portfolio to your business?

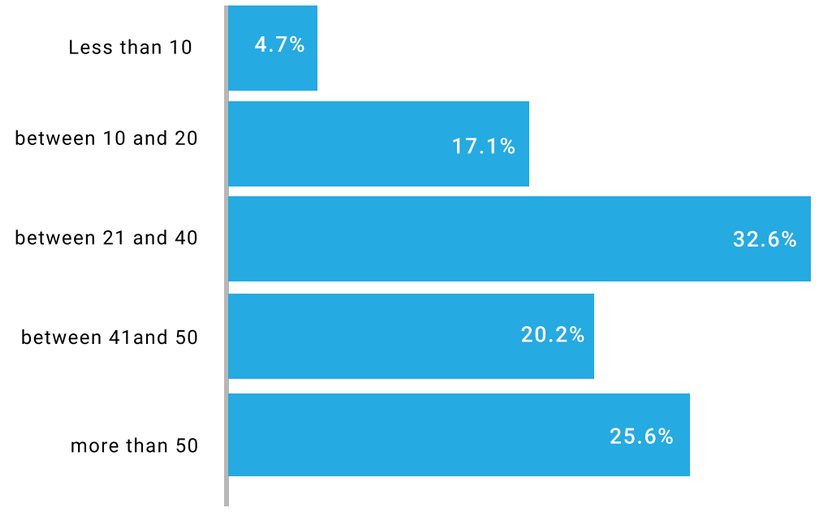


We learned:

Enterprises in Cameroon consider an application portfolio to be essential for their business and that it provides them a competitive advantage.

We asked:

What is the size of your application (in-house built and commercial) (e.g: outlook, sagesaari, MS Excell, …) portfolio?

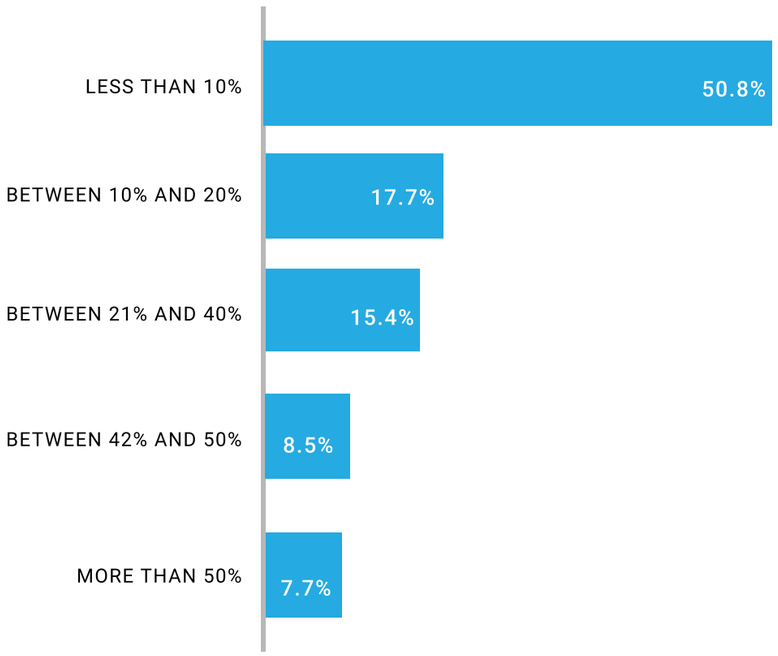


We learned:

A significant proportion of enterprises have between 21 - 40 applications in their portfolio

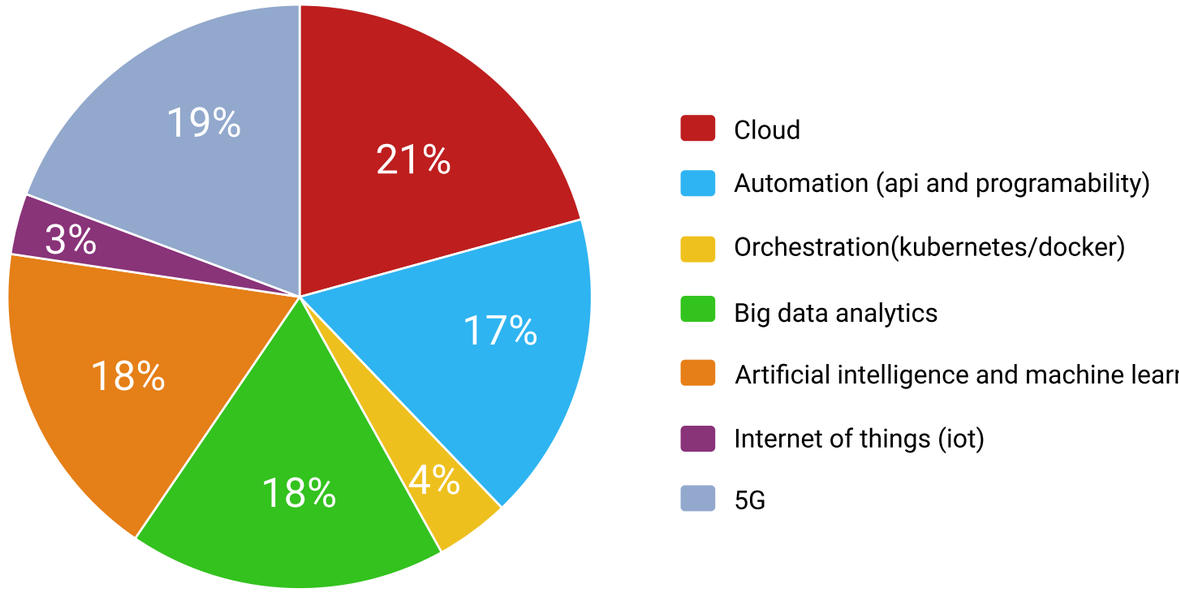
We asked:

What is the percentage of in-house built application ?



We asked:

Which technology trends do you think will be strategically important for you over the next 2-5 years?



We learned:

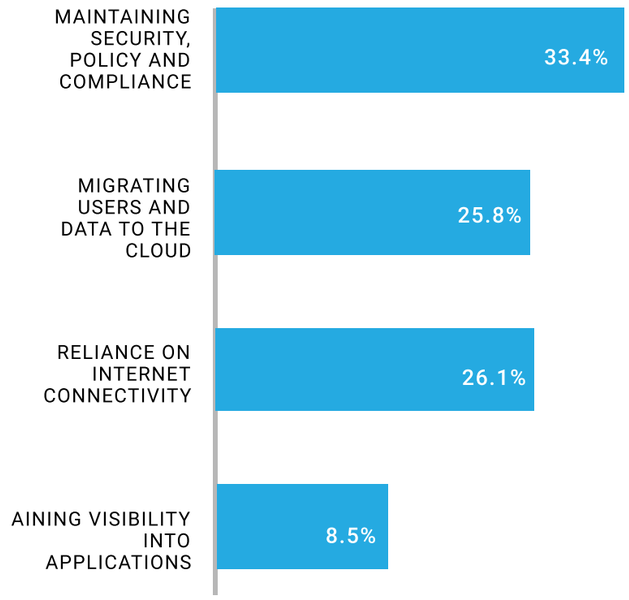
Most enterprises generally outsource the development of their applications.

We learned:

Cloud computing currently leads as the most strategically important tech trend, though AI, Big Data and Automation are also considered strategically important by enterprises in Cameroon.

We asked:

As you think about migrating applications into the Cloud, what parts of managing the application do you find the most challenging, frustrating, or difficult?

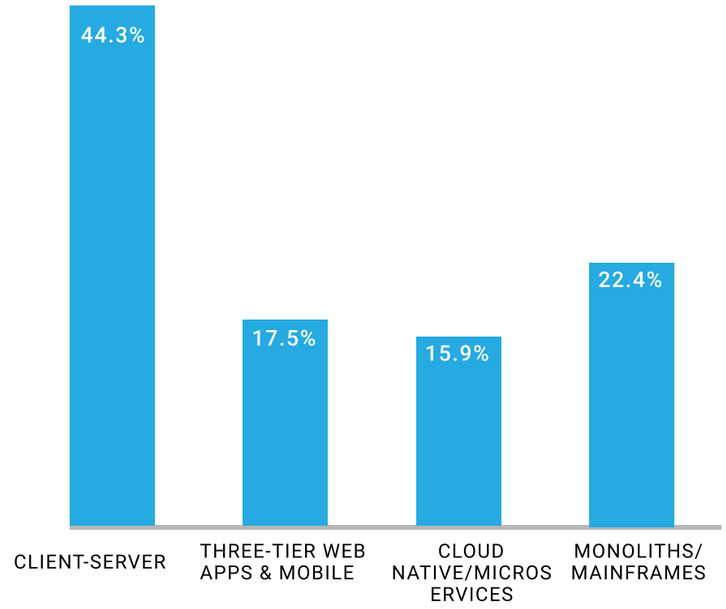


We learned:

Maintaining security, policy and compliance is most challenging to enterprises Cameroon when migrating their applications to the Cloud.

We asked:

Illustrate the current application deployment map in your organisation ?

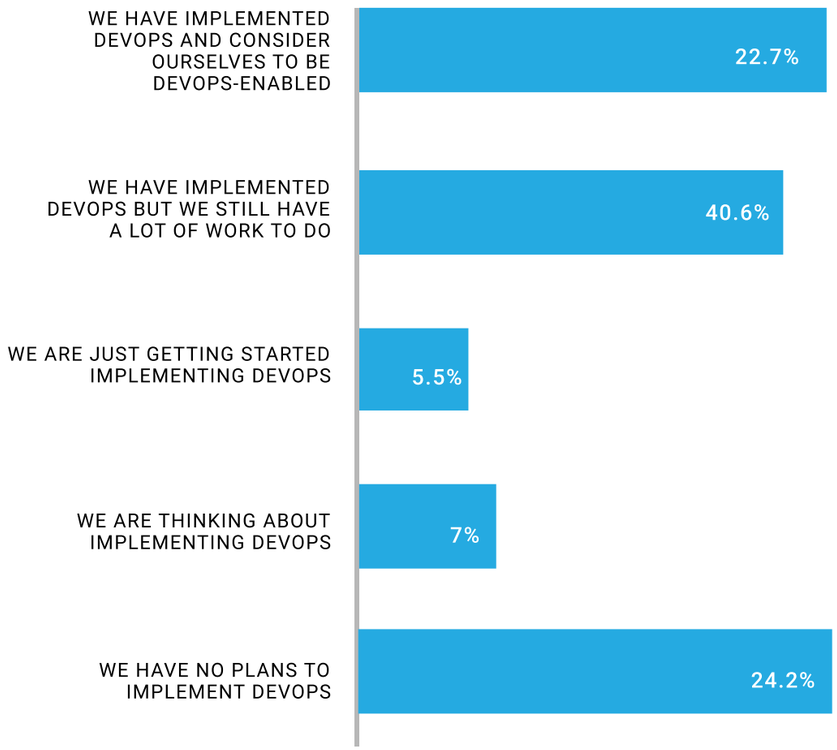


We learned:

Client-Server application architectures are most common in Cameroon.

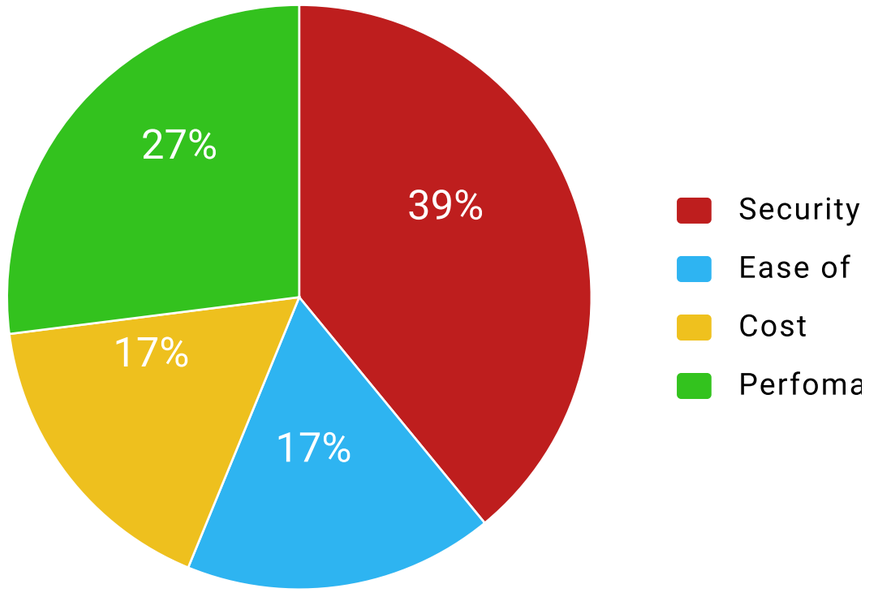
We asked:

How far along is your organization in its DevOps journey?



We asked:

When deploying an application, please select your first and second most important concern.



We learned:

Most organizations are at the very early stages of their DevOps journey

We learned:

Most organizations worry most about the security of an application during deployment.

A significant number of respondents also worry about the performance of the application.

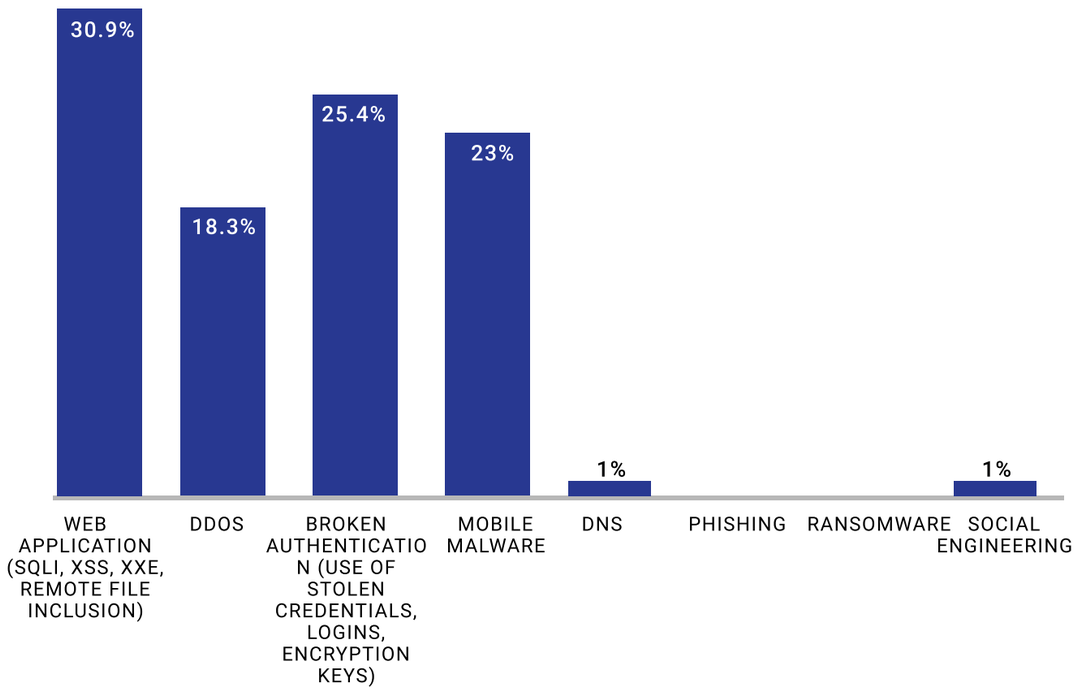
Threat attack surface and trend

56.3% of enterprise apps and data threat attack surface is from Web application attacks such as SQLi, XSS, XXE, and RCE and to Broken authentication leading to Fraud.

The vast majority of respondents are most fearful of data loss or data leak as a result of an exploit. Moreover, security is increasingly becoming a concern as 66.6% of respondents say they have noticed an increase in threats over the past 12 months.

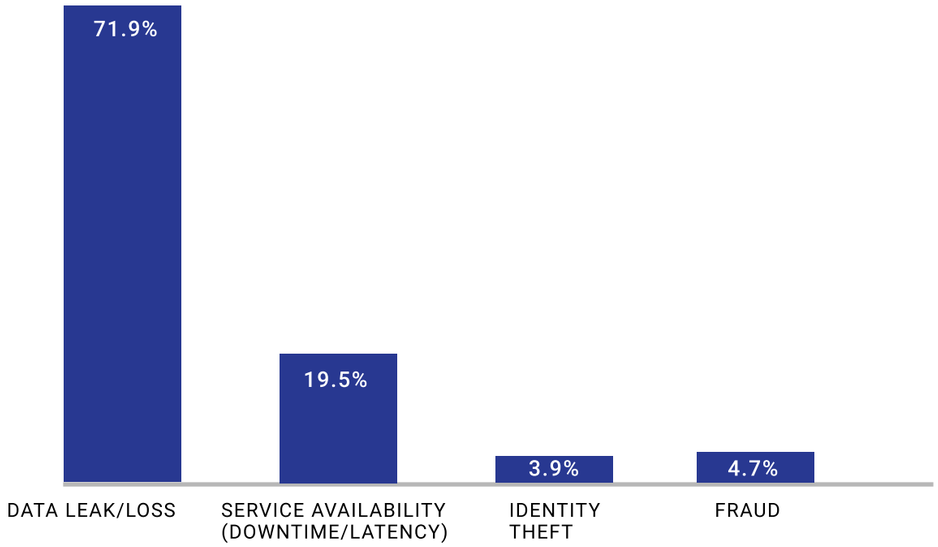
We asked:

How are external attacks carried out against your application ?



We asked:

What are you the most afraid of ?



We learned:

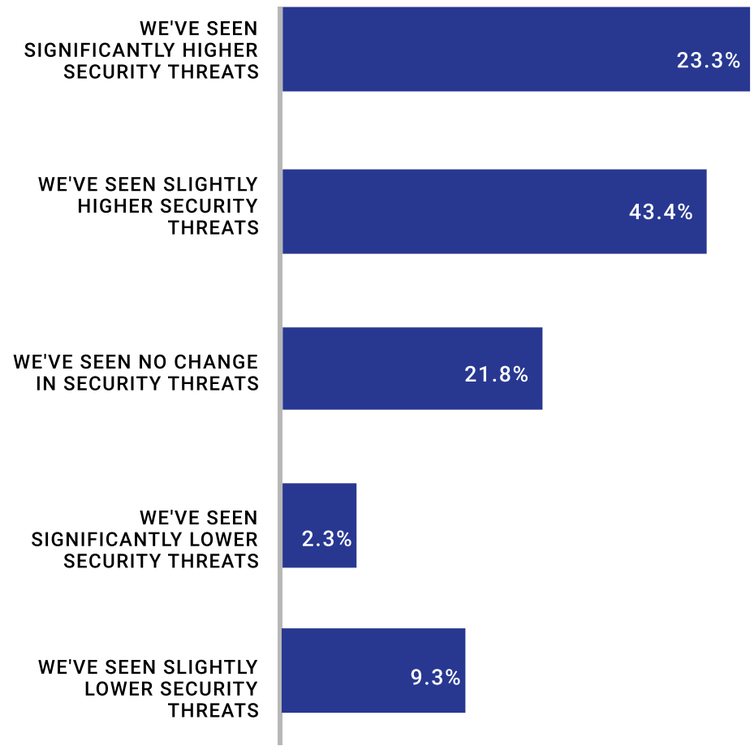
Most external attacks are through web applications

We learned:

Enterprises in Cameroon are most afraid of a leak or loss of data.

We asked:

Has your organization seen a difference in the number of security threats in the past 12 months ?

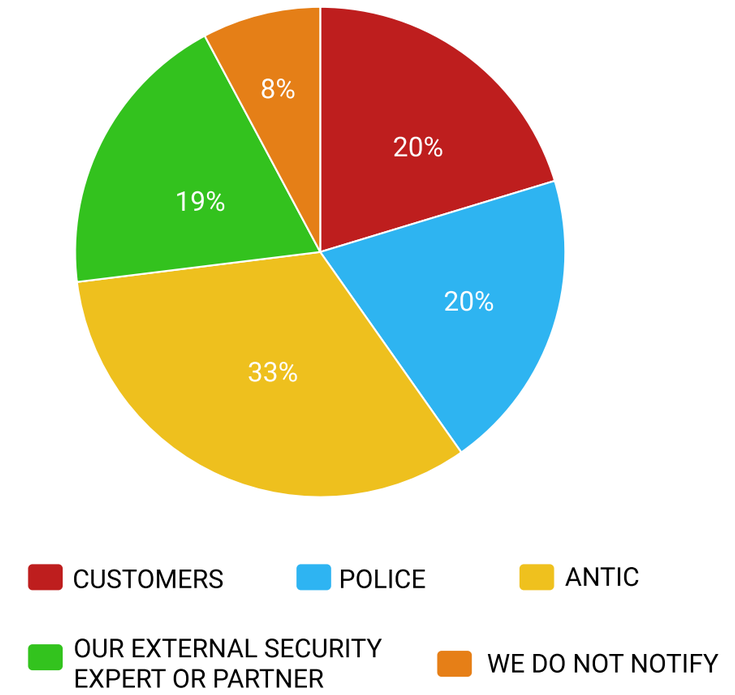


We learned:

A few organizations have seen significantly higher security threats in the last 12 months but in general, there has been only a slight increase of security attacks on enterprises in Cameroon in the last 12 months.

We asked:

To whom does your organization notify stakeholders of security attacks against its applications?

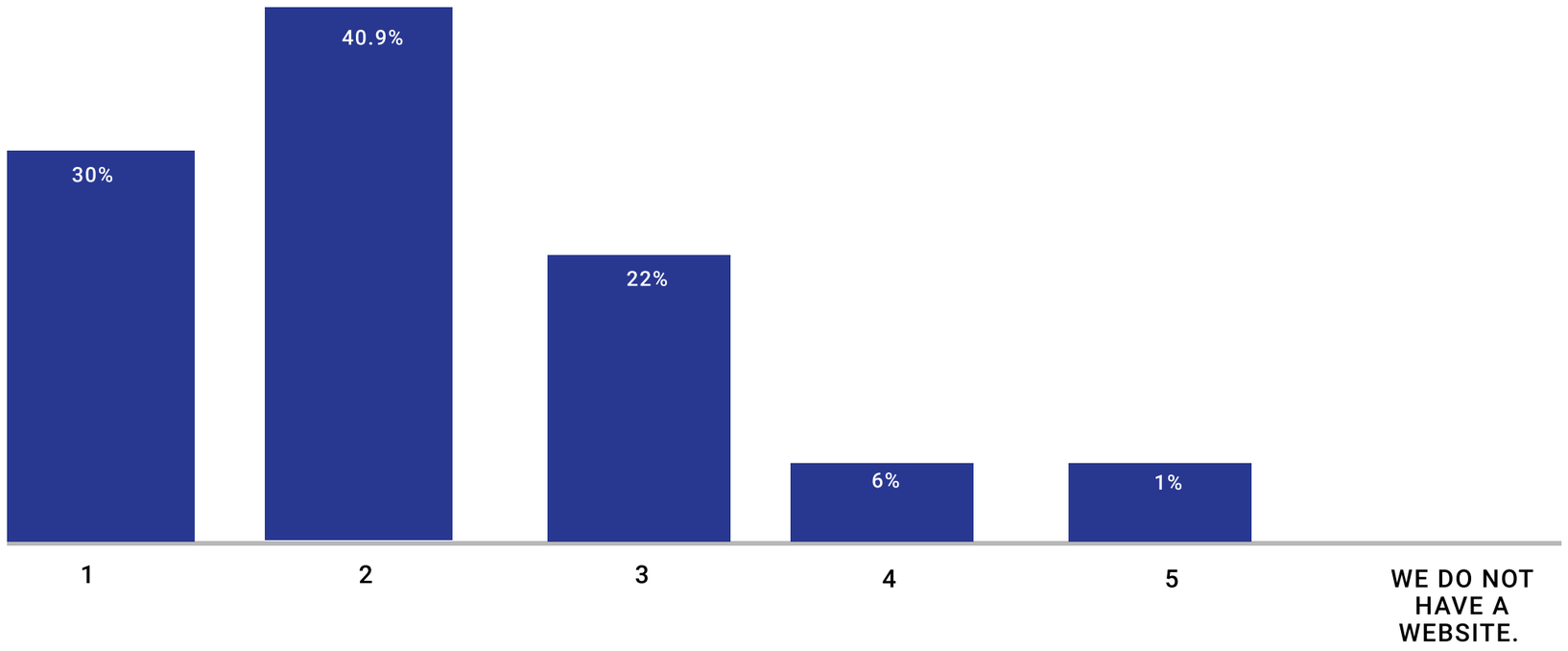


We learned:

Only a few enterprises in Cameroon notify customers of a security breach. They mostly notify the regulator ANTIC.

We asked:

What is the level of vulnerability of your organization website ?



We learned:

Most enterprises consider their website vulnerability to be medium.

Organizations security readiness

16% of enterprises had a Web Application Firewall. Moreover, only 8.4% performed Penetration Testing.

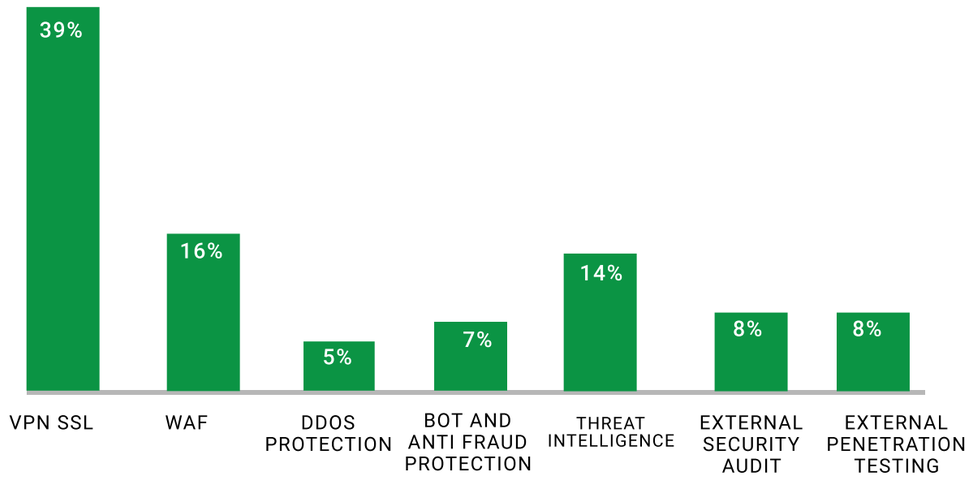
This points to the fact that majority of enterprises still focus on security at the network level and that a lot still needs to be done by enterprises in Cameroon in terms of their application security readiness.

71% thought that ensuring the security of customer information was most important regarding application security. Meaning customers' data protection is a priority for most enterprises.

While a security breach would speed up the security buying process for most enterprises, more than 85% said they use in-house application security solutions and testers.

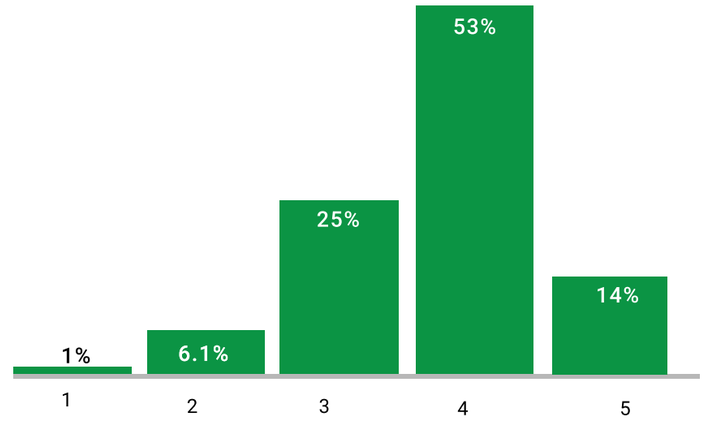
We asked:

Which of the following security services does your organization currently deploy ?



We asked:

On a scale of 1-5 (with 1 being lowest and 5 being highest) how confident are you in your company's ability to withstand an attack against your applications ?



We learned:

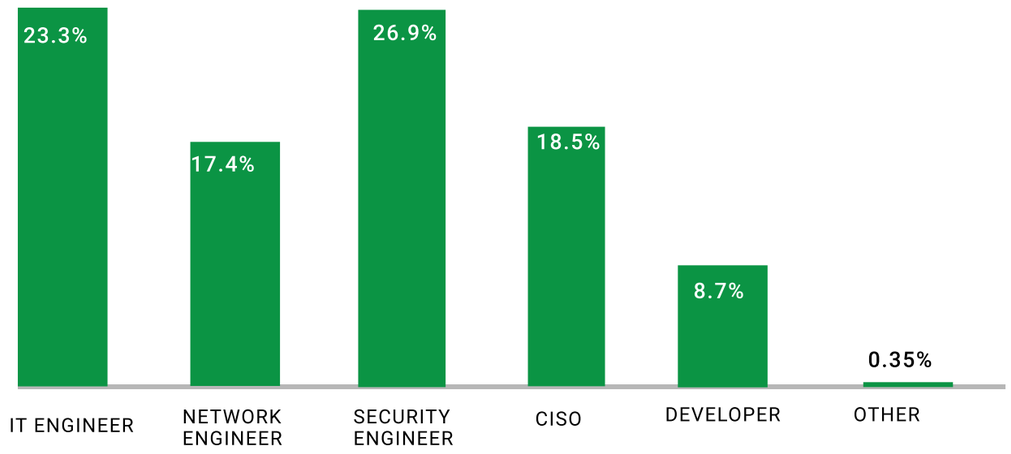
Enterprises in Cameroon focus on network level security like SSL VPNs

We learned:

Enterprises are falsely confident of their ability to withstand an attack against their applications, taking into consideration their responses on measures taken to secure their applications.

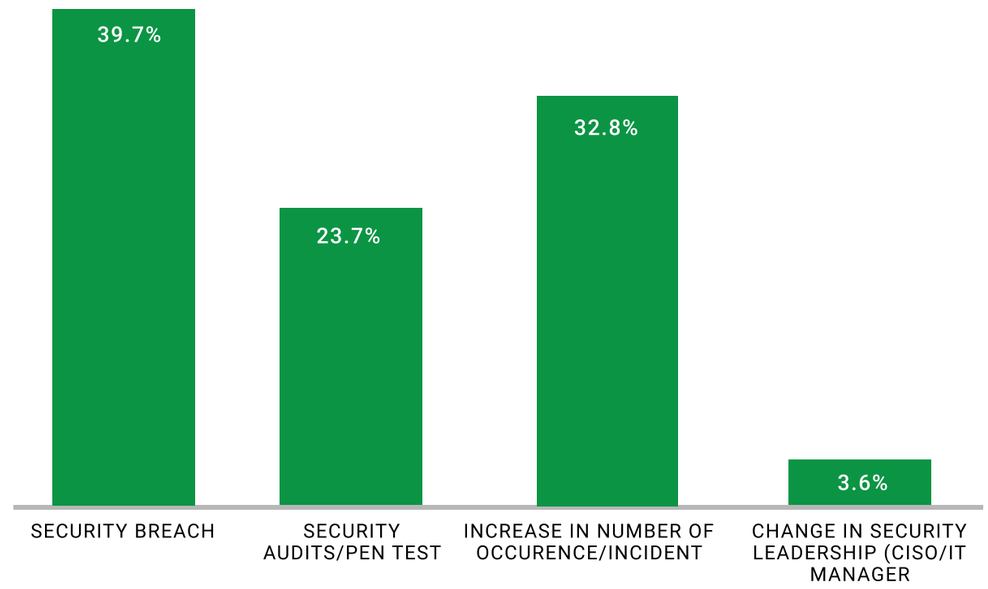
We asked:

Which roles within your organization are primarily responsible for securing your applications ?



We asked:

What events “speed up” the need, and buying process, for security solutions?



We learned:

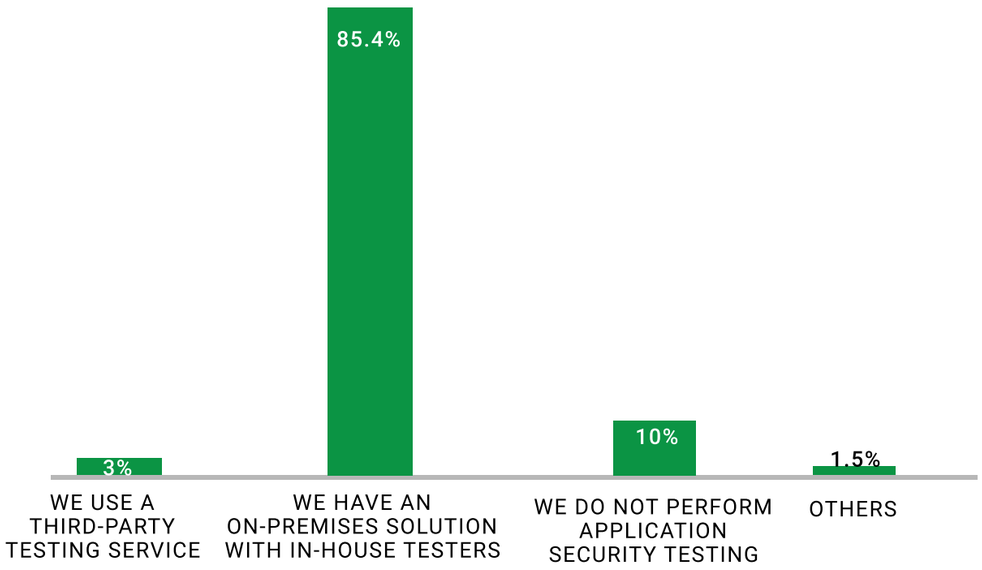
Most enterprises do not hire a security engineer to secure their systems. They let their regular IT team do the security job.

We learned:

Enterprises admit a security breach or increase in number of Incidents rather than a change in leadership of the IT department will speed up security spending decisions.

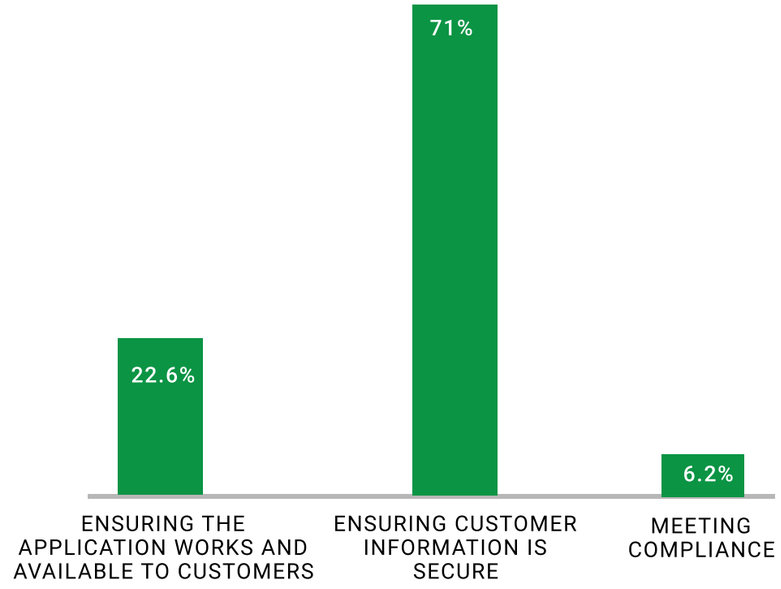
We asked:

How does your organization currently manage application security testing?



We asked:

What do you consider to be most important regarding application security?



We learned:

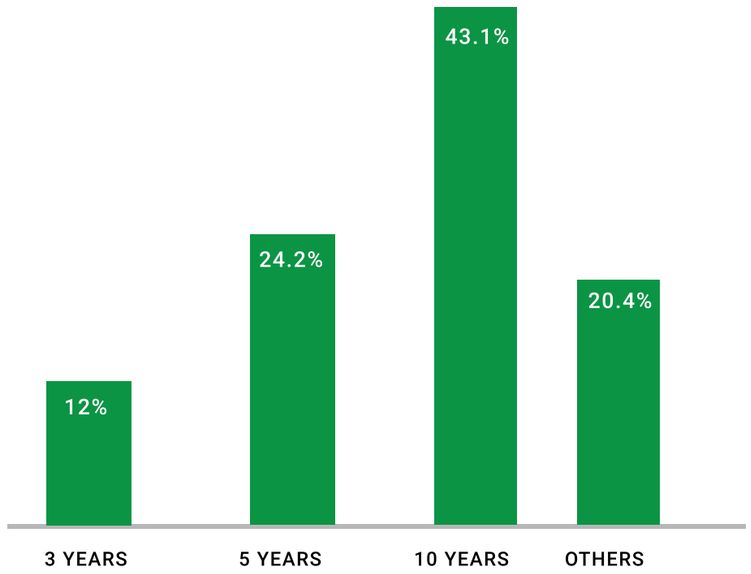
The internal IT team performs application security testing for the majority of enterprises.

We learned:

The security of customer data is what enterprises in Cameroon consider the most important in application security.

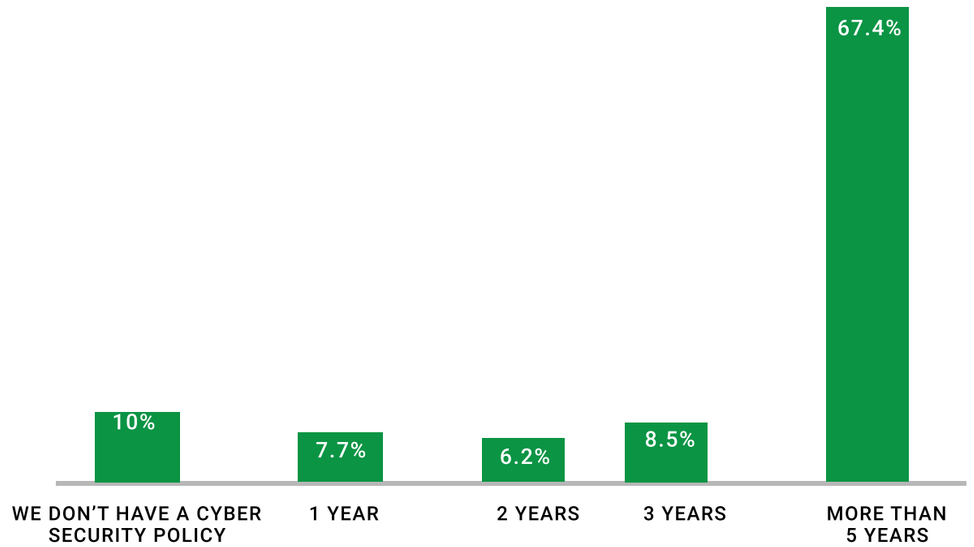
We asked:

How long do you keep operational and traffic data in your organization ?



We asked:

How long have you had a cyber security policy ?



We learned:

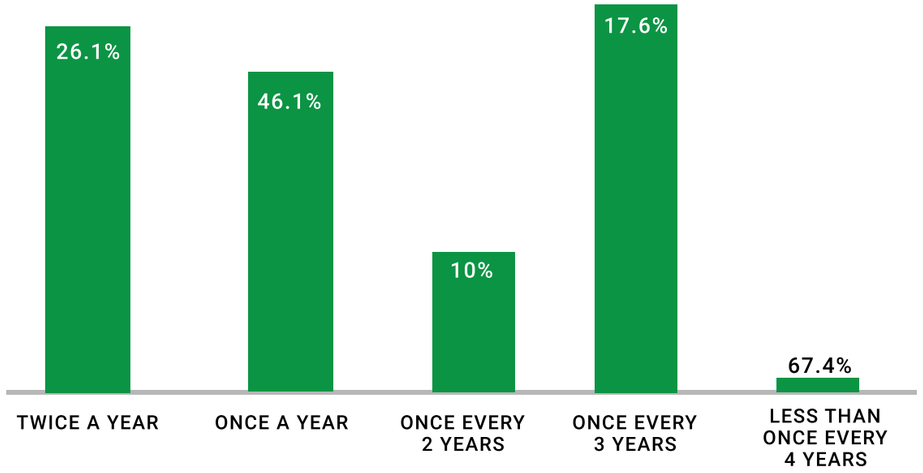
It is common to keep operational data for up to 10 years in Cameroon.

We learned:

Most enterprises have had a cybersecurity policy for more than 5 years while a few said they had none.

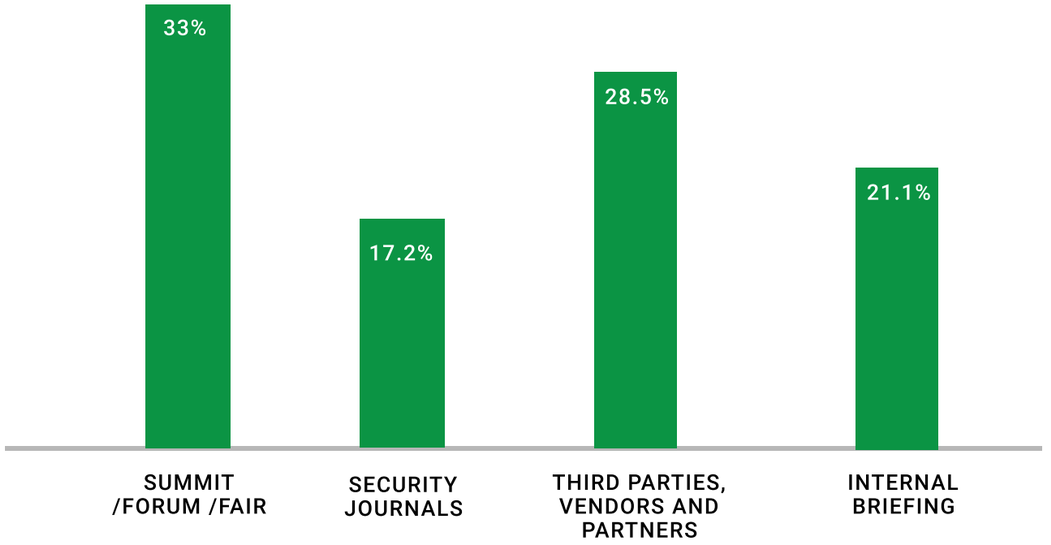
We asked:

How often does your organisation perform cybersecurity audit ?



We learned:

How does your organization keep updated with security threats and solutions ?



We learned:

Most enterprises perform a cybersecurity audit once a year.

We learned:

Seminars and summits are the primary way enterprises in Cameroon keep up to date with security threats and solutions.

Regulation of application security

39.2% of enterprises said they used the local National Agency for Information & Communication Technologies (ANTIC) standards and an equal percentage of enterprises use the ISO27001 standard.

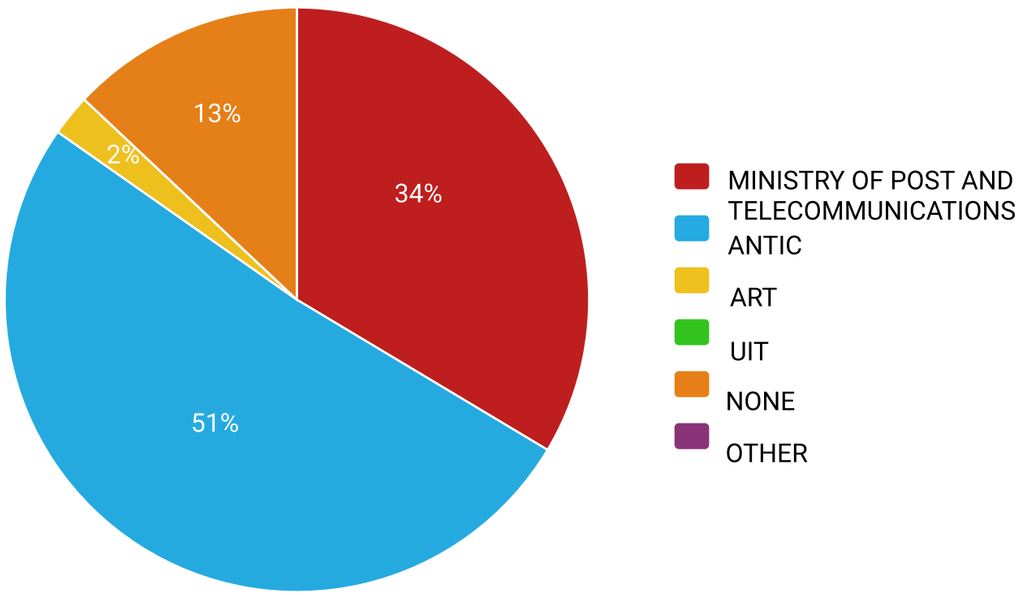
This would explain why 51.1% of enterprises said they collaborate with ANTIC than any other regulatory body in the country.

Only 3.6% of enterprises interviewed do not use PKI infrastructure to secure their applications, which is a good sign in terms of security awareness in the country. SSL certificates signed by ANTIC are as common as DIGICERT and SYMANTEC signed certificates.

40.3% of respondents said they use the security vendor Cisco and 30.6% use Checkpoint solutions.

We asked:

Amongst the following institution, which one does your organization collaborating with ?

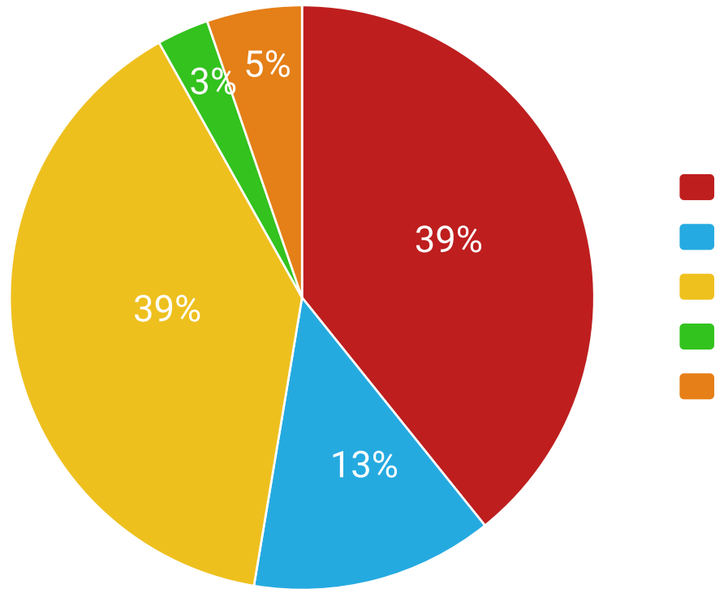


We learned:

Enterprises in Cameroon mostly collaborate with the local regulator ANTIC

We asked:

Which regulations or standards does your organization apply ? Select all that apply.

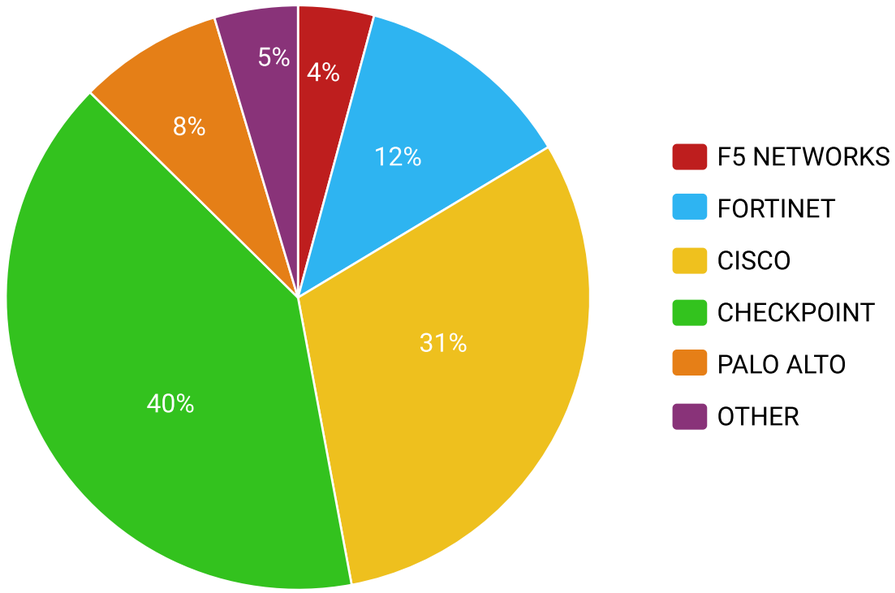


We learned:

The standards and regulation commonly complied within Cameroon are ANTIC and ISO27001.

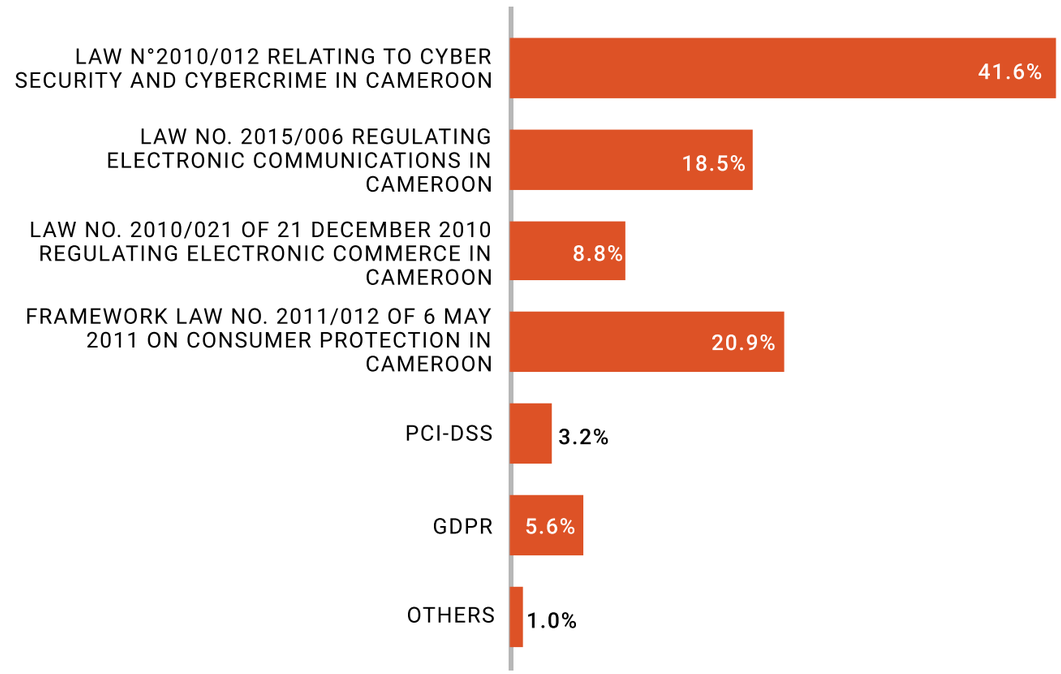
We asked:

Who are your application security vendors?



We asked:

Among the following regulations, give the ones you usually use



We learned:

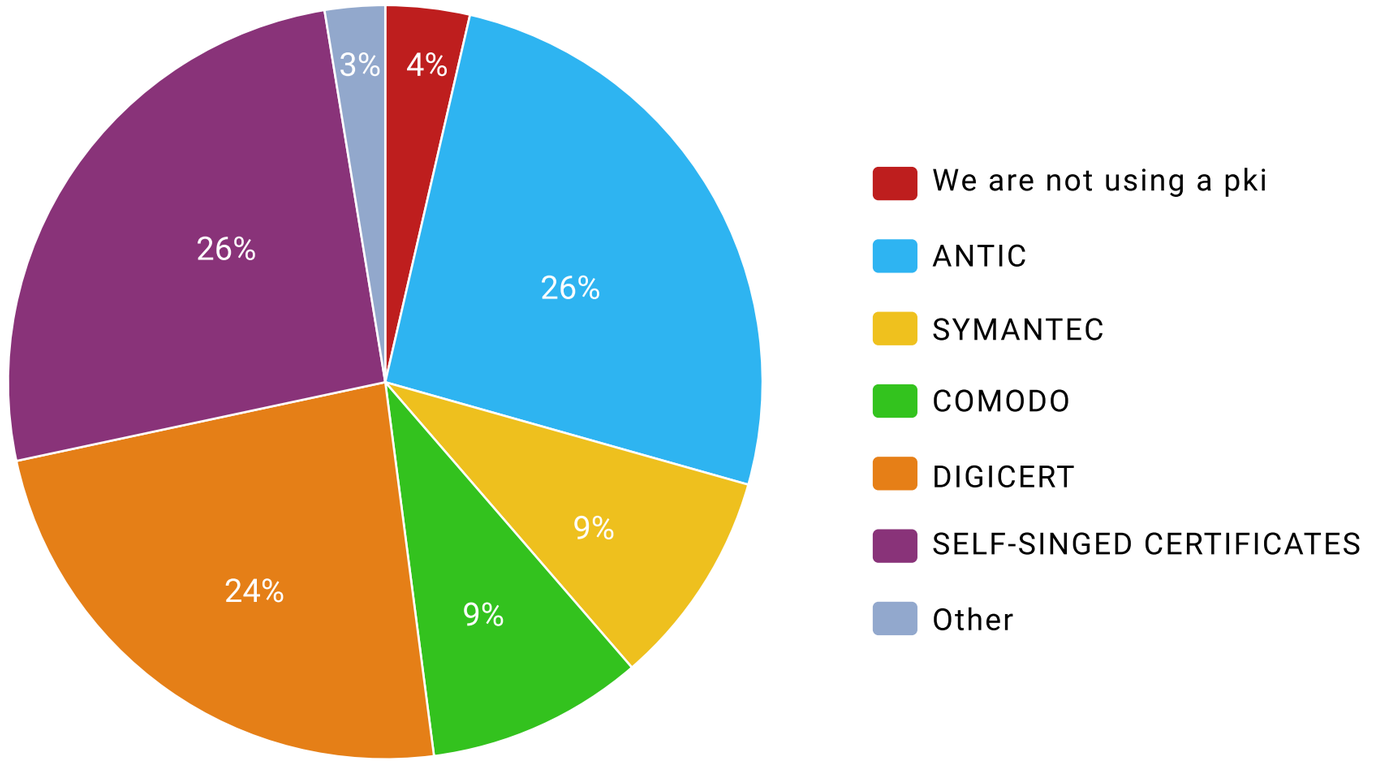
Cisco has approximately 40% of the security market share, followed by Checkpoint with about 30.6%.

We learned:

Enterprises seek to comply with Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime in Cameroon more than any other law. And only about 5% of enterprises comply with the EU's GDPR.

We asked:

Which Certificate Authority do you use to protect your data and applications ?



We learned:

ANTIC and Digicert signed certificates are commonly used in Cameroon. Only a very few did not use PKI or self-signed certificates.

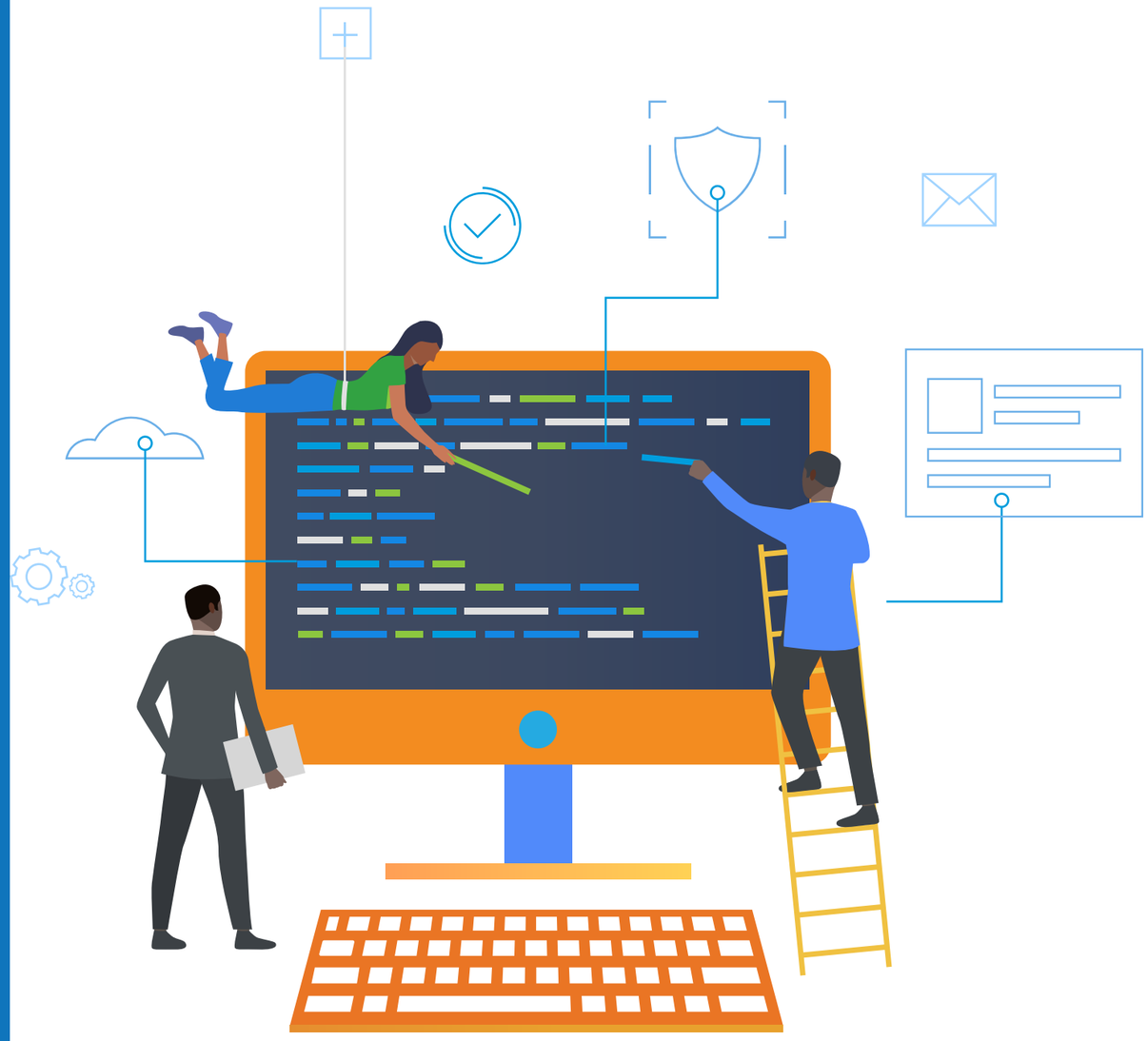
III. Conclusion

In this study, we set out to answer three main questions:

- How does the threat attack surface and trend in Cameroon look like?
- How are organizations' security readiness?
- And how does regulation of application security look like in Cameroon?

From the results of the study, it is clear that while enterprises in Cameroon are aware of security threats and risks to their systems in general, they do not pay much attention to application level security. The study shows that most enterprises seem to still focus on network level security, leaving their applications vulnerable to hacking attacks and exploitation. As a result, the Open Web Application Security Project (OWASP) top 10 attacks and broken authentication are pertinent with a huge potential for Fraud and data loss/leak. A possible reason for this is that most enterprises are at the early stages of their DevOps journey and the dominance of monolithic application architectures in enterprises. This presents an opportunity not only for awareness raising in organizations, but also an opportunity for growth in revenue for both the Cameroonian cybersecurity sector and security vendors.

Furthermore, the study showed that with regards to compliance to information security standards and regulations, most enterprises focus on compliance with the local standards and regulations. While this is expected, the very low compliance rate with or focus on other regulations like the European General Data Protection Regulation (GDPR) might point to a low service offering to non-Africans and business dealings with consumers from outside the continent.



Annex I: Research Methodology and Sampling

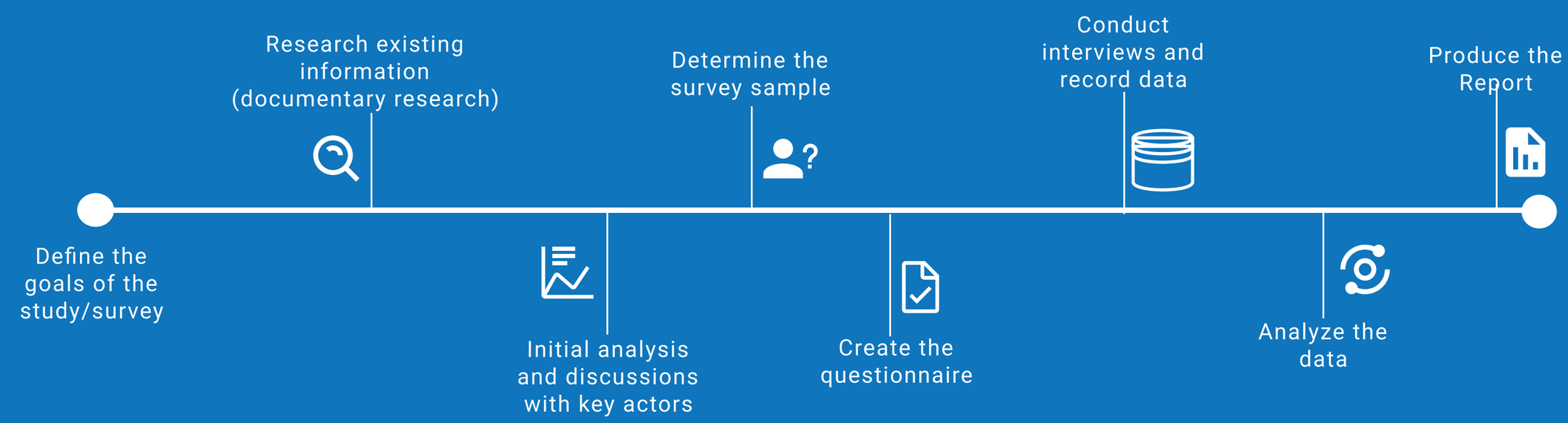
Research Methodology

This study started with a documentary research to understand Cameroon's enterprise digital security ecosystem while collecting available information and identifying information gap. We summarized the findings of the documentary research in the article **WEB SPACE: SOMMES NOUS EN SECURITE ?** published at www.gefona.org. Following the documentary study, we organized formal and informal discussions with key actors in Cameroon's cyberspace to further refine the study and perceive initial trends.

We then designed a questionnaire in order to survey the current state of digital security affairs, confirm initial trends and supply missing information. We used a combination of online (social media & emails), telephonic and in-person (face2face) interviews. From the information collected during the interview, we analyzed the data and extracted insights.

While Cameroon consists of 28872 businesses, only 1.5% employing 100+ personnel[4]. We define an enterprise as organizations in the private or public sector with 100+ employees. The findings in this report are based on a survey of 42 private and pubic enterprises across the 2 major cities (Douala and Yaounde) in Cameroon, from which we got 137 responses.

Generally, our research methodology is as follow:



ANNEX II: REFERENCES

[1] Government of Cameroon. 2010/2020 Growth and Employment Strategy paper.
https://www.cameroonembassyusa.org/mainFolder/images/documents_folder/quick_links/Cameroon_DSCE_English_Version_Growth_and_Employment_Strategy_Paper_MONITORING.pdf

[2] McAfee (2018). Economic Impact of Cybercrime—No Slowing Down. Retrieved from
https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

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

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