Global Scientific JOURNALS
GSJ: Volume 10, Issue 5, May 2022, Online: ISSN 2320-9186
www.globalscientificjournal.com

IMPACT OF SECURITY TOOLS ON DATA SECURITY IN CAMEROON

Dr Djousse Hugues Marceluce [1*], Fondem Princess Nkenganang [2], Tchouante Christelle Grace [2]
Institut Africain d'Informatique (IAI CAMEROUN),software engeeniering ;
ICT University department des systemses d'information et reseaux
*Auteur correspondant **: Email : consultingtic32@gmail.com**

Abstract

In a world where cyber-security is a major concern and data is fast becoming a key asset, safeguarding this asset is a primary responsibility. This has brought about a massive demand and influx in security tools for the monitoring, detection and response of threats and vulnerabilities. Due to exponential increases in variations of security threats and even higher volumes of sensitive data, organizations in Cameroon have begun employing the use of multiple security tools to deal with specific problems. The attitudes and practices of people and organizations using this tools have implications on the confidentiality, availability and integrity of data. This paper provides a brief overview of the impact of Security Tools on Data Security in Cameroon. Through this paper, we want to provide our perspective on the positive and negative effects that may be brought about by the use of security tools during the implementation of data security. We then analyze our data, describe our findings, reflect on our results, discuss better security practices and provide our direction on future research.

Keywords: **cyber-security, data, threats, attacks and vulnerabilities, data security, monitoring, detection and response, security tools**.

resumé

Dans un monde où la cybersécurité est une préoccupation majeure et où les données deviennent rapidement un actif clé, la sauvegarde de cet actif est une responsabilité primordiale. Cela a entraîné une demande et un afflux massifs d'outils de sécurité pour la surveillance, la détection et la réponse aux menaces et aux vulnérabilités. En raison

de l'augmentation exponentielle des variations des menaces de sécurité et des volumes encore plus élevés de données sensibles, les organisations camerounaises ont commencé à utiliser plusieurs outils de sécurité pour faire face à des problèmes spécifiques. Les attitudes et les pratiques des personnes et des organisations utilisant ces outils ont des implications sur la confidentialité, la disponibilité et l'intégrité des données. Ce document donne un bref aperçu de l'impact des outils de sécurité sur la sécurité des données au Cameroun. A travers cet article, nous souhaitons donner notre point de vue sur les effets positifs et négatifs que peut entraîner l'utilisation d'outils de sécurité lors de la mise en place de la sécurisation des données. Nous analysons ensuite nos données, décrivons nos conclusions, réfléchissons à nos résultats, discutons de meilleures pratiques de sécurité et fournissons notre orientation pour les recherches futures.

Mots clés : cyber-sécurité, données, menaces, attaques et vulnérabilités, sécurité des données, surveillance, détection et réponse, outils de sécurité.

1. Introduction

Society and economic development in general continues to rely heavily on information systems and networks in Africa. Almost all sectors, whether agriculture, finance, education or government, all increasingly depend on information and communication technology to enable solutions.

Many businesses, including those with models not common in Africa are being built to support this new paradigm of economic development in many countries on the

continent. At the same time, security threats enabled by ICT are growing at an alarming rate and the threat actors themselves are evolving. A remote farmer who would traditionally only be worried about attacks from local robbers, now have to worry about the availability of the platform from which s/he accesses markets and the security of a digital wallet. Reports of billions of dollars lost by businesses and individuals to cyber-crime are becoming a common feature in the media. Even more worrying besides the financial losses is that systems and networks providing critical services to societies are also at risk of attack and sabotage. Fortunately, some businesses are taking advantage of this phenomena to develop tools that monitor systems and applications. in order to detect and respond to cyber-threats, therefore ensuring data protection (privacy and security). Over the years, the continuous use of these tools have shown an increase in threat mitigation. protection and recovery of sensitive data across Africa. However, such data is hard to find on the continent. Where there is some data, the studies focus primarily on the English-speaking countries like Nigeria. Ghana and South Africa . For this reason, we set out to study the usage of and attitude towards security tools in Cameroon.

Data security tools are tools or software designed to secure all types of data, from individual messages to entire databases. Data security should always be a priority for both individuals and companies in order to keep our data safe. However, there are speculations that data privacy comes at a price to data security which leads us to question the overall "goodness" of these tools. Thus, we need to understand these tools, starting with an understanding of what organizations perceive as security tools, data security, their readiness to address the identified threats and regulatory compliance to both international and local standards.

2. Literature Overview

Following the topic of this study, we have as main target Cameroon which is very broad or quite narrow. It is important to carefully explain the methodology used to collect data from a vast population for the realization of this study.

2.1. Methodology

The data used for this study was collected using sub-methods from both Probability random sampling and Non-Probability sampling**.** In this project we used simple random sampling and clustered sampling from probability sampling in combination with the judgement and bias sampling from non-probability sampling. The choice of methodology is based on the fact that Cameroon is constituted of few security companies/bodies that are more concentrated in the Center and Littoral regions. So we chose random companies/persons/IT specialists located in both regions based on their expertise and previous experiences in the domain. Simple random sampling was applied at the level where we had a group of companies with similar roles and employee numbers and had to make a choose on which ones will be a sample for this study and later on, used the results to produces our sample clusters of two companies. Moreover, we rushed into the judgement and bias sampling because most Cameroonians in these areas and as a whole lack knowledge on security tools and data security. So, a judgement was made on those with better experience in the security domain to get quick, concurrent and accurate data used for the article.

In addition to the probability and non-probability sampling methods, another method through which information for the realization of this paper was collected is the **SLR** (**Systematic Literature Review**) methodology. We had to review relevant literature in our field of study and go through it rigorously to get the analytical methods used in those papers and sources. So as to be in line with the writer and have a better understanding of the points and facts raised by the writers in our resources.

2.2. Data Analysis

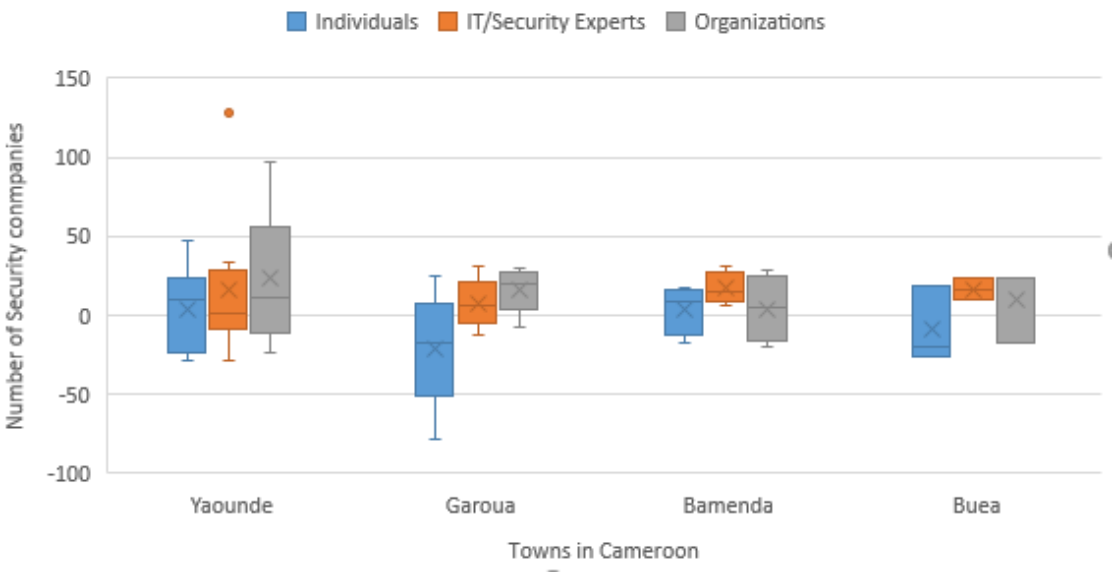


Figure 1: Distribution of Security Tool users in Cameroon.

For the purpose of this study. the diagram above shows statistics of security tool users in different towns (found in different regions) in the country. It is seen that Yaounde has the highest number of people and organizations implementing data security procedures. Most of these people have used at least two security tools in all of their computer devices. Organizations with multiple systems and applications that are local or on the cloud have used as much as 10-30 security tools. With the increasing number of threats and vulnerabilities, many of these individuals and organizations are of the opinion that security tools have had and will continue to have only positive effects on their data security. However, more than half of these entities' understanding of security tools are limited to antivirus, scanning and response software. Using these observations, we then outline the findings/results of this study.

3. Results

3.1. Perceived Benefits

There is no doubt that security tools have helped mitigate and stop millions of threats to computer systems and applications. From our research and analysis, it is perceived that the most popular security tools are antivirus and web scanning software. Although more organizations have begun to warm up to these tools, there exists a certain level

and ignorance and distrust when it comes to security. Fortunately software like QualysGuard and HP WebInspect provide organizations with the ease of use, centralized management and integration capabilities they need to keep the attackers at bay and their web applications secure. This provides and all-in-one solution for organizations by enabling incidence response, vulnerability management and disaster recovery. To further show the benefits of security tools, we use QualysGuard and HP WebInspect as tools of reference:

3.1.1. QualysGuard

i. KEY FEATURES

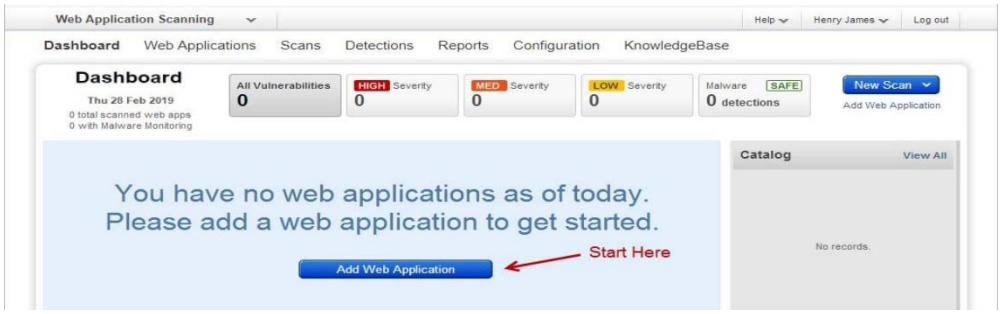
- Crawl web applications (Intranet, Internet) and scan them for vulnerabilities
- Fully interactive UI with flexible workflows and reporting
- Identify web applications' handling of sensitive or secret data
- Customize: black/white lists, robots.txt, sitemap.xml and more
- Supports common authentication schemes
- View reports with recommended security coding practice and configuration

ii. ROBUST SCALABLE SCANNING CAPABILITIES

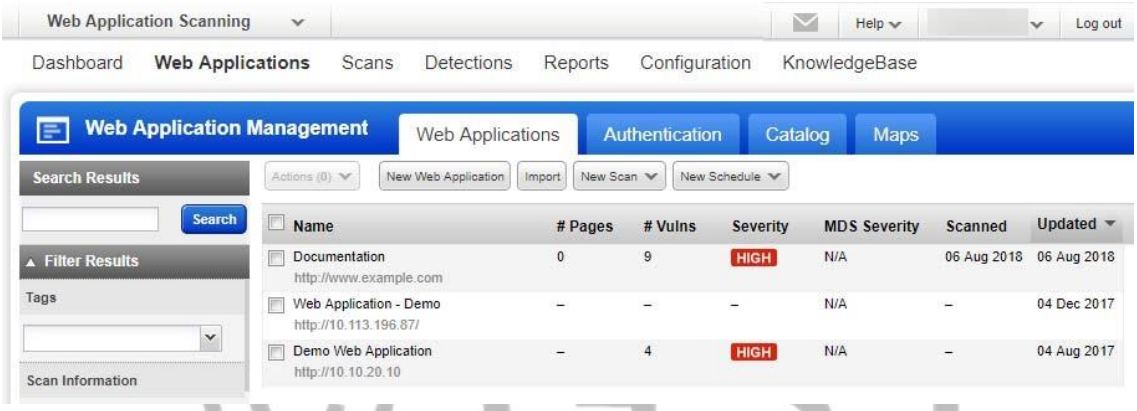
- Supports scanning HTML web applications with JavaScript and embedded Flash
- Comprehensive detection of custom web application vulnerabilities including OWASP Top 10 Vulnerabilities
- Differentiates exploitable fault-injection problems from simple information disclosure - Profiles custom web application behaviors
  Configures scanning performance with customizable performance level

iii. HOW THE APPLICATION WORKS

- Here, the user enters the web application (name or URL) that needs to be scanned.

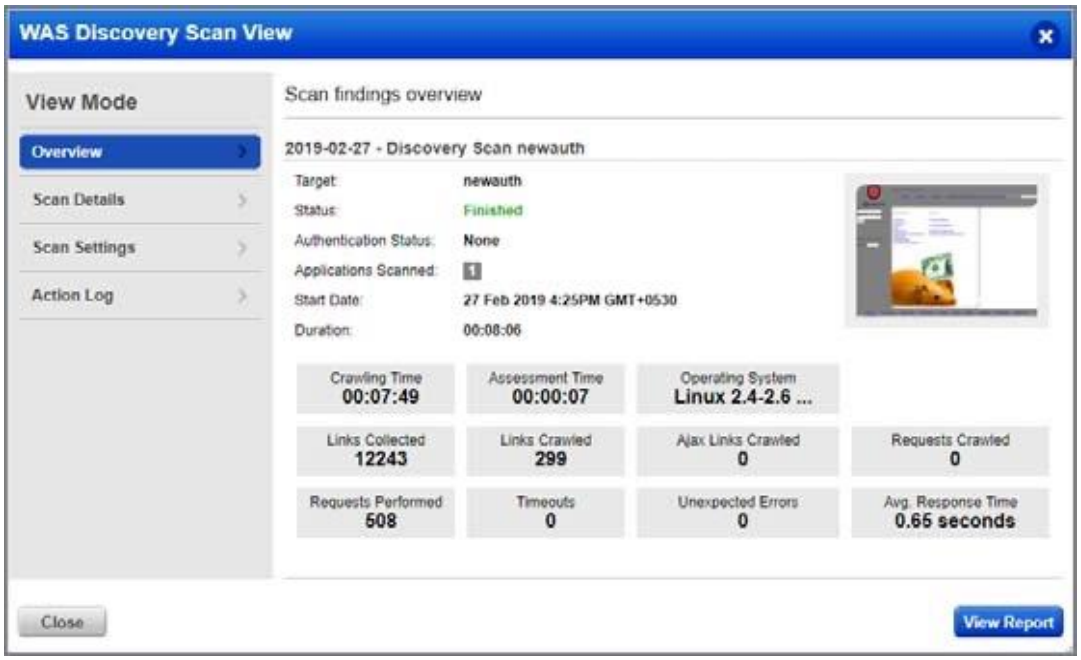


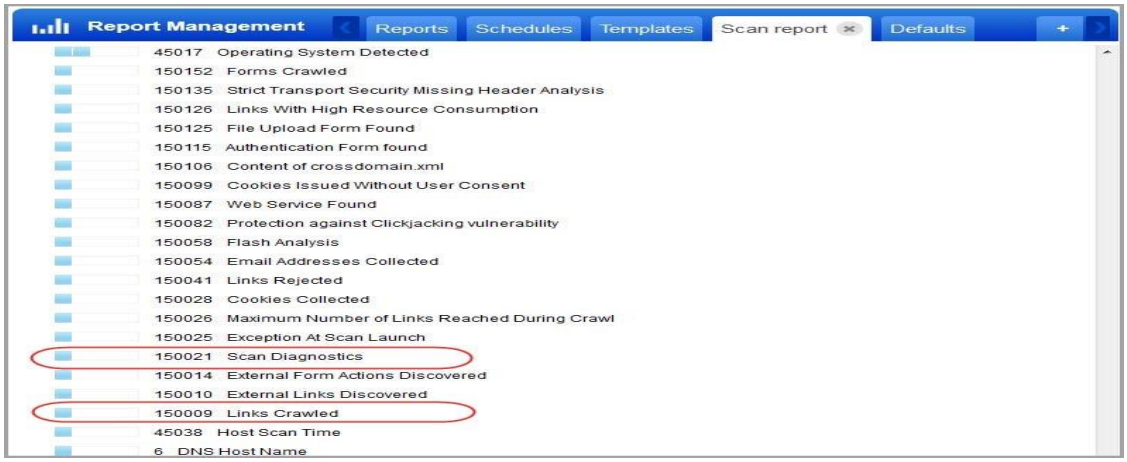
- The web application appears in the Web Applications tab, where application



settings can be edited or a scan on it is launched.

- **The scan view:** The Overview provides an overview of the scan findings where the full scan report is generated.



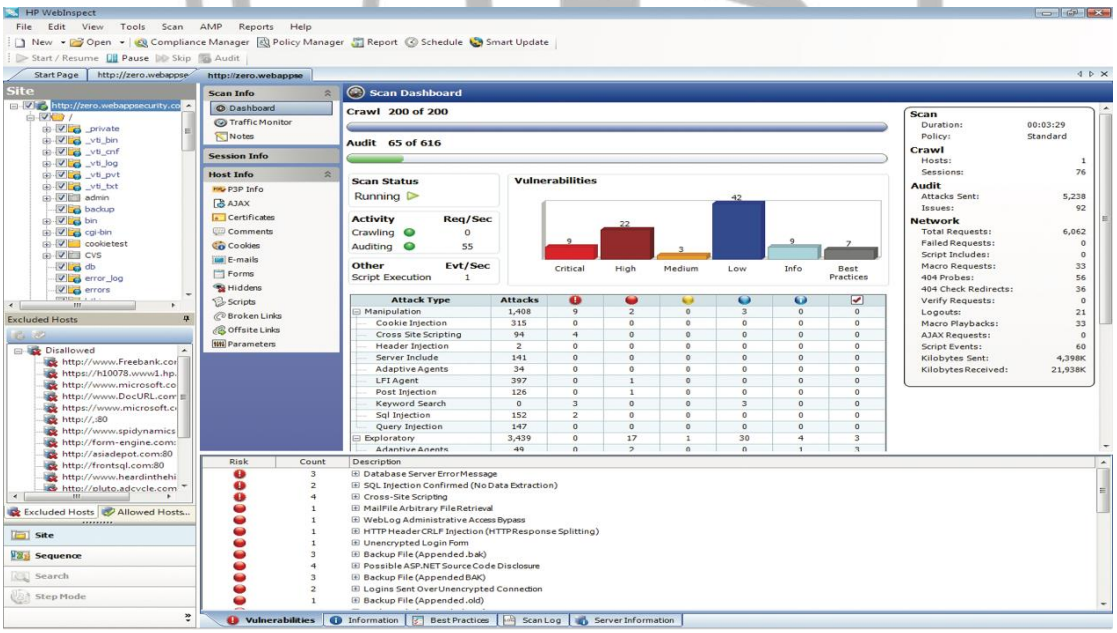


- **The full scan report:** Each QID is a security check that was performed.

3.1.2. HP WebInspect

HP WebInspect is the industry leading Web application security assessment solution designed to thoroughly analyze today's complex Web applications and Web services for security vulnerabilities.

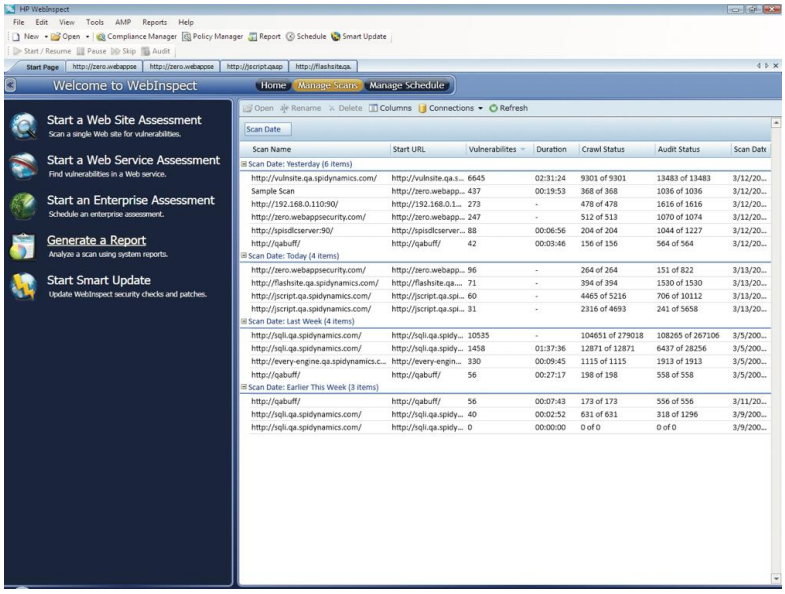
i. WEBINSPECT SCAN DASHBOARD



Dashboard delivers real-time visibility into and interactivity with test results

ii. WEBINSPECT SCAN DATABASE

Easily manage, view and share your security test results and history



Looking at all of the features of of these it is to be believed that data security is becoming better and more automated. However, some concerns were raised concerning data privacy and the surveillance nature of these software. Thus, we provide an overview of the probable consequences and hesitation towards these tools.

3.2. Hesitation Towards Security Tools

Most organizations using security tools in Cameroon have very little to barely adequate knowledge of security, much less security tools which brings up the concern of their misuse. Cameroon as a developing country faces “software and security poverty”; thus, the general population can afford to get cheap security tools that perform just the bare minimum. Because of how expensive security tools can be, millions of installed antivirus and auditing software that have the full functionalities have been downloaded from sketchy sites. Many of these come with third-party monitoring software and unfortunately, even government employees fall prey to these sites leading to data breaches and loss of information.

It is common knowledge that many of these software have servers internationally causing concerns over data localization which could give other nations access to sensitive data that could be used in cyber-warfare.

The continuous use of these tools leads to alert fatigue sometimes, caused by false positives. This is detrimental as many security threats are caused by ignorance and

human mistakes. Time and resources are wasted on multiple tools posing more risk to data security.

From these points, it can be deduced that security tools pose a big threat to the nation's data security as a whole especially with the fact that there aren't enough good regulations and policies on cyber-security in Cameroon. This could be the reason towards the low number of organizations in Cameroon adopting this technology as opposed to others.

Conclusion

Security tools are important for many organizations in the developing world. In this study we focused on QualysGuard and WebInspect which are some powerful security tools use for vulnerability management.

A high proportion of organizations in Cameroon face online attacks and are increasingly concerned with their safety in digital spaces. However many of this internet users are unaware of any legal protection offered to them. Additionally, they believe that they lack the appropriate knowledge to protect themselves in these digital spaces. Results from the analysis show that there is a significant need in security tools aimed at building data security awareness. Security tools can be trusted, but only in the right hands. With better policies and regulation aimed towards this domain, these tools greatly increase the security of the nation as a whole.

The main limitation of this work come from fact that there was not enough accurate data to best produce this study. As stated in the Methodology section, most statistics on security in African countries are geared towards those countries with a higher economy, computer literacy and those moving towards adopting cyber-security regulations as a whole. Out of 54 countries, only 13 of them have taken this positive step forward and unfortunate, Cameroon is not one of them. We believe that this study could be done better with more researchers and better access to data. In the future, we would like to go deeper into these tools' influences and how thy can be improved for th good of the country.

References

- Qualys web application scanning : http://www.hp.com/hpinfo/newsroom/press_kits/2011/risk2011/HP_WebInspect_data_sheet.pdf
- HP WebInsPect : http://www.hp.com/hpinfo/newsroom/press_kits/2011/risk2011/HP_WebInspect_data_sheet.pdf
- https://libraryguides.griffith.edu.au
- https://www.scribbr.com
- https://www.jotform.com
- https://allafrica.com/stories/202011050461.html
- https://accelerationeconomy.com/cybersecurity/cybersecurity-tool-sprawl-can-lead-to-team-overload-and-lower-impact/
- https://cipesa.org/2019/09/overview-of-cameroons-digital-landscape/
- https://www.digitaldefense.com/blog/reducing-the-negative-impact-of-security-on-iot-ics/
- https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/
- https://gefona.org/state-of-cyberspace-security-in-africa/
- https://www.sciencedirect.com/science/article/pii/S2352728516300677
- https://www.researchgate.net/publication/317968117_The_rise_of_cybersecurity_and_its_impact_on_data_protection
- https://www.sciencedirect.com/science/article/pii/S1877050919305915