الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعليم العالي و البحث العلمي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Centre de Recherche
Sur l'Information Scientifique et Technique

مركز البحث
في الإعلام العلمي والتقني

RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de

Post Graduation Spécialisée en Big Data et Calcul Intensif

Plateforme Big Data pour la cybersécurité

Réalisé par : BENYDIR Rabie & SALHI Lotfi

Encadreur : Mme NOUALI Nadia & Mr YAHIAOUI Said

Soutenu le :00/07/2019. **Devant le jury** composé de :

Président : Mr. KABOU Abdelbasset

Examinateurs : Mr. GEMRAOUI Lila

Mr. DERKI Mohamed Sadek

Année Universitaire : 2018 /2019

ملخص

أصبح الأمن السيبراني من أهم مجالات معالجة البيانات الضخمة، لأن حجم وتعقيد البيانات المتعلقة بالأمن السيبراني أصبح كبيرًا جدًا بحيث لا يمكن معالجتها بواسطة الأدوات والوسائل التقليدية. بالإضافة إلى ذلك، هناك مجموعة كبيرة من أدوات معالجة البيانات الضخمة المستخدمة في الأمن السيبراني والتي يتم انتقاؤها حسب الواقع.

في هذا العمل، نقترح معالجة إشكالية إنشاء أرضية خاصة بالأمن السيبراني تستند على أدوات معالجة البيانات الضخمة، بطريقة مستنيرة تعتمد على دراسة الهدف المسطر والمعلومات المتوفة حاليا. حيث قمنا بإجراء دراسة مقارنة لمختلف الأرضيات المتوفرة حاليا والمتعلقة بالأمن السبرياني وبشكل أكثر تحديداً، أدوات المعالجة الخاصة بالبيانات الضخمة، سمحت لنا هذه الدراسة المقارنة بتسليط الضوء على معايير الاختيار لتصميم حل يتناسب ومتطلبات التطبيق المقصود.

في النهاية، ولشرح الوضع في الخدمة لنظام خاص بالأمن السيبراني قائم على أدوات معالجة البيانات الضخمة من الناحية العملية، قمنا بتصميم ووضع في الخدمة لتطبيق يتمثل في مراقبة تدفق بيانات الشبكة حيث يتم أولا التقاط وحفظ البيانات بصفة آنية، بعدها يتم تحليلها وعرضها مع اظهار حالة استغلال الشبكة.

Abstract

Cybersecurity is becoming a Big Data problem along with the growing size and complexity of security data that cannot be manipulated by traditional security tools. In addition, there is panoply of Big Data tools proposed for use in cybersecurity and choosing the right ones is not so straight.

In this work, we propose to treat the problem of setting up a Big data-based cybersecurity platform, in as knowledgeable as possible way, after an objective and well-documented study of the solutions proposed in the current state of the art. Thus, we made a comparative study of existing Big Data platforms dedicated to cybersecurity and more specifically, tools dedicated to the Big Data procecessing. This comparative study allowed us to highlight selection criteria for the design of a solution that is adapted to the requirements of the intended application.

At the end, and to explain in practical terms the implementation of a cybersecurity platform based on Big Data, we implemented a network traffic monitoring application consisting in capturing and saving, in real time, the network flow, and then making some analysis and visualization on the collected data to give an image on the network status.

Résumé

La cybersécurité est en train de devenir un problème de Big Data en raison de la taille et de la complexité croissante des données de sécurité qui ne peuvent pas être manipulées par les outils de sécurité traditionnels. De plus, il existe une panoplie d'outils Big Data proposés pour la cybersécurité et choisir les bons dépend de la réalité.

Dans ce travail, nous proposons de traiter le problème de la mise en place d'une plateforme Big Data de cybersécurité basée sur les données, de la manière la plus informée possible, après une étude objective et bien documentée des solutions proposées dans l'état actuel des connaissances. Nous avons donc réalisé une étude comparative des plates-formes Big Data existantes dédiées à la cybersécurité et plus particulièrement des outils dédiés au traitement du Big Data. Cette étude comparative nous a permis de mettre en évidence des critères de sélection pour la conception d'une solution adaptée aux besoins de l'application envisagée.

Enfin, pour expliquer concrètement la mise en place d'une plateforme de cybersécurité basée sur le Big Data, nous avons implémenté une application de surveillance du trafic réseau consistant à capturer et à sauvegarder, en temps réel, le flux du réseau, puis à effectuer des analyses et une visualisation sur les données collectées mettant en évidence l'état d'utilisation du réseau.

Table des matières