الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 08. ماي 1945. بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **Engineer**
Field: **Computer science**
Specialty: **Information Systems and Web (SIW)**

Theme

Towards a SIEM for Personal Data Protection at Djezzy

Presented by:
Boukharouba Yahia
Cherrab Mohamed abdelkarim

Submission Date: **June, 2024**
In front of the jury composed of:

Dr. Malki Abdelhamid	President
Dr. Khaldi Miloud	Examiner
Dr. Awad Samir	Supervisor

Academic Year : 2023/2024

Abstract

The big advancements of the internet and it's various benefits have made it a must to rely on for every single enterprise.Also, because of the technology popularity in the last few years, security risks have become a serious concern, with cyber-attacks increasing every day. As a result, a company must continuously check and monitor its security status in order to take corrective and responsive actions quickly. SIEM and SOAR systems work together in a security operation center (SOC) to provide organizations with a comprehensive view of security status and protect their IT infrastructure.

Furthermore, the protection of personal data has become the priority "0" in today's digital world. To avoid any harm for personal information, organizations must follow severe data protection standards and adopt many strict strategies . In Algeria, personal data protection is guaranteed by Law 18-07, which presents strict data privacy and security measures. This law emphasizes the necessity of putting in place strong strategies to protect the confidentiality, integrity, and availability of personal information.

This research report discusses cutting-edge SIEM systems that are commonly employed. This includes both open-source and proprietary solutions. There is currently no complete SIEM system architecture accessible, as reported in the literature. This research proposes a comprehensive, well-defined, and modular design for SIEM system for Djezzy enterprise. Each module was thoroughly detailed, including input parameters, processing, and output details. This modular approach allows developers to increase SIEM system features without compromising performance or integration, while also assisting end users in making informed judgments about SIEM system selection. Also, the proposed architecture prioritizes compliance with data protection legislation, guaranteeing that the system not only improves security but also meets legal criteria for personal data protection.

Key Words: SIEM, SOAR, Personal data protection, Confidentiality, Security

Résumé

Les avancées remarquables d'Internet et ses nombreux avantages l'ont rendu crucial pour presque toutes les entreprises. À mesure que la technologie devient plus populaire et largement utilisée, les risques de sécurité deviennent une préoccupation majeure, avec une augmentation de la fréquence des attaques. Par conséquent, une entreprise doit vérifier en permanence son état de sécurité afin de prendre des mesures correctives rapides. Les systèmes SIEM et SOAR travaillent ensemble dans un centre d'opérations de sécurité (SOC) pour fournir aux organisations une vue complète de l'état de sécurité et protéger leur infrastructure informatique.

De plus, la protection des données personnelles est devenue une priorité absolue dans le paysage numérique actuel. Pour préserver les informations personnelles, les organisations doivent suivre des normes de protection des données strictes. En Algérie, la protection des données personnelles est régie par la loi 18-07, qui établit des exigences strictes en matière de confidentialité et de sécurité des données. Cette loi souligne la nécessité de mettre en place des mesures solides pour protéger la confidentialité, l'intégrité et la disponibilité des informations personnelles.

Ce rapport de recherche discute des systèmes SIEM de pointe couramment utilisés. Cela inclut les solutions open-source et propriétaires. Il n'existe actuellement aucune architecture de système SIEM complète disponible, comme le rapporte la littérature. Cette recherche propose une conception complète, bien définie et modulaire pour le système SIEM pour l'entreprise Djezzy. Chaque module a été détaillé de manière exhaustive, y compris les paramètres d'entrée, le traitement et les détails de sortie. Cette approche modulaire permet aux développeurs d'augmenter les fonctionnalités du système SIEM sans compromettre les performances ou l'intégration, tout en aidant les utilisateurs finaux à prendre des décisions éclairées sur le choix du système SIEM. De plus, l'architecture proposée privilégie la conformité à la législation sur la protection des données, garantissant que le système améliore non seulement la sécurité mais répond également aux critères légaux de protection des données personnelles.

Mots-clés : SIEM, SOAR,Protection des données personnelles, Confidentialité, sécurité

ملخص

إن التطورات الملحوظة والفوائد العديدة للإنترنت جعلته ضروريًا لكل مؤسسة تقريبًا. ومع زيادة شعبية التكنولوجيا واستخدامها على نطاق واسع، أصبحت المخاطر الأمنية مصدر قلق كبير مع تزايد الهجمات بشكل متكرر. ونتيجة لذلك، يجب على الشركة فحص حالتها الأمنية باستمرار لاتخاذ إجراءات تصحيحية سريعة. تعمل أنظمة SIEM و SOAR معًا في مركز عمليات الأمن (SOC) لتزويد المؤسسات برؤية شاملة لحالة الأمان وحماية بنيتها التحتية لتكنولوجيا المعلومات.

علاوة على ذلك، أصبح حماية البيانات الشخصية أولوية قصوى في المشهد الرقمي اليوم. للحفاظ على المعلومات الشخصية، يجب على المؤسسات اتباع معايير حماية البيانات الصارمة. في الجزائر، تحكم حماية البيانات الشخصية القانون رقم 07-18، الذي يضع متطلبات صارمة لخصوصية وأمن البيانات. يؤكد هذا القانون على ضرورة وضع تدابير قوية لحماية سرية وسلامة وتوافر المعلومات الشخصية.

تتناول هذه الدراسة أنظمة SIEM المتطورة التي تُستخدم بشكل شائع. يتضمن ذلك الحلول مفتوحة المصدر والحلول التجارية. لا توجد حاليًا بنية شاملة لنظام SIEM متاحة كما هو مذكور في الأدبيات. تقترح هذه الدراسة تصميمًا شاملاً ومحددًا ومودوليًا لنظام SIEM لمؤسسة دجيزي. تم تفصيل كل وحدة بدقة، بما في ذلك معلمات الإدخال، والمعالجة، وتفاصيل الإخراج. يسمح هذا النهج الموديلي للمطورين بزيادة ميزات نظام SIEM دون التأثير على الأداء أو التكامل، مع مساعدة المستخدمين النهائيين أيضًا في اتخاذ قرارات مستنيرة بشأن اختيار نظام SIEM. أيضًا، يعطي التصميم المقترح الأولوية للامتثال لتشريعات حماية البيانات، مما يضمن أن النظام لا يحسن الأمان فقط بل يفي أيضًا بالمعايير القانونية لحماية البيانات الشخصية.

الكلمات المفتاحية: SIEM، SOAR، حماية البيانات الشخصية، السرية، الامن