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 **Master**
Field: **Computer Science**
Specialty: **Information Systems and Web (SIW)**

Theme

An Overview of SIEM Approaches

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 Internet technology knows a tremendous growth in the last few years which has transformed businesses 360 degrees, because it provides new prospects for growth and innovation. However, this digitalization or digital revolution led to the appearance of cyber threats, posing substantial challenges to the security of key assets and data in today's rapidly expanding digital ecosystem.

In order to respond to these challenges, Businesses are increasingly relying on strong security measures and technics to protect their IT infrastructures and guarantee and preserve the integrity and confidentiality of their data. One of these measures is the implementation of a Security Information and Event Management (SIEM) system, which acts as a single hub for monitoring and analysing security-related events and occurrences.

This thesis gives a complete overview, evaluation, and categorization of current SIEM solutions, it will also explains how SIEM's can improve their ability to meet new security challenges and prove compliance with the regulatory standards. The study will focus on the strengths and limits of different SIEM solutions, as well as the essential aspects impacting their effectiveness, through an in-depth examination of credible papers and platforms.

By shedding light on these issues, the study hopes to help informed decision-making in selecting the best SIEM solution for an organization's specific needs. The thesis intends to provide stakeholders with the knowledge and insights they need to properly traverse the complicated environment of cybersecurity solutions by thoroughly examining SIEM functionality, features, and performance metrics.

Finally, the study aims to contribute to the cybersecurity world discussion by trying to provide some valuable insights about the SIEM solutions and their evolving role in protecting organizations from cyber threats and ensuring the security of their digital infrastructure in an increasingly interconnected world.

Keywords : Internet technology, Cyber threats, Security measures, SIEM, IT infrastructure, Regulatory compliance, Security challenges, Data integrity, Decision-making, Cybersecurity solutions, Performance metrics, Information security, Threat detection, Risk management

Résumé

Les avancées rapides de la technologie internet ces dernières années ont transformé la façon dont les entreprises fonctionnent, offrant de nouvelles perspectives de croissance et d'innovation. Cependant, cette révolution numérique a entraîné une prolifération des cybermenaces, posant des défis substantiels à la sécurité des actifs clés et des données dans l'écosystème numérique en pleine expansion d'aujourd'hui.

En réponse à ces difficultés, les entreprises s'appuient de plus en plus sur des mesures de sécurité solides pour protéger leur infrastructure informatique et préserver l'intégrité et la confidentialité des données sensibles. Une de ces mesures est le déploiement d'un système de gestion des informations et des événements de sécurité (SIEM), qui agit comme un hub unique pour surveiller et analyser les événements et les incidents liés à la sécurité.

Cette thèse vise à donner un aperçu complet, une évaluation et une catégorisation des solutions SIEM actuelles, en mettant l'accent sur leur capacité à relever les défis de sécurité modernes et à se conformer aux normes réglementaires. L'étude a pour objectif de mettre en lumière les forces et les limites des différentes solutions SIEM, ainsi que les aspects essentiels influençant leur efficacité, à travers une analyse approfondie de documents et de plateformes crédibles.

En éclairant ces questions, l'étude espère aider à prendre des décisions éclairées dans le choix de la meilleure solution SIEM pour les besoins spécifiques d'une organisation. La thèse a pour but de fournir aux parties prenantes les connaissances et les idées nécessaires pour naviguer correctement dans l'environnement complexe des solutions de cybersécurité en examinant en profondeur les fonctionnalités, les caractéristiques et les métriques de performance des SIEM.

Enfin, cette étude vise à contribuer à la discussion en cours sur la cybersécurité en fournissant des informations précieuses sur le rôle évolutif des solutions SIEM dans la protection des organisations contre les menaces émergentes et en assurant la résilience de leur infrastructure numérique dans un monde de plus en plus interconnecté.

Mots-clés : Technologie internet, Cybermenaces, Mesures de sécurité, SIEM, Infrastructure informatique, Conformité réglementaire, Défis de sécurité, Intégrité des données, Prise de décision, Solutions de cybersécurité, Métriques de performance, Sécurité de l'information, Détection des menaces, Gestion des risques

ملخص

لقد حول التقدم السريع في تكنولوجيا الإنترنت في السنوات الأخيرة طريقة عمل الشركات، مما وفر فرصًا جديدة للنمو والابتكار. ومع ذلك، فقد أدى هذا التحول الرقمي إلى انتشار التهديدات السيبرانية، مما يشكل تحديات كبيرة لأمن الأصول الأساسية والبيانات في النظام الرقمي المتسارع النمو في الوقت الحالي.

استجابةً لهذه الصعوبات، تعتمد الشركات بشكل متزايد على تدابير أمنية قوية لحماية بنيتها التحتية لتكنولوجيا المعلومات والحفاظ على سلامة وسرية البيانات الحساسة. إحدى هذه الخطوات هي نشر نظام إدارة معلومات وأحداث الأمان (المعلومات الأمنية ونظام إدارة الأحداث)، والذي يعمل كمركز واحد لمراقبة وتحليل الأحداث والحوادث المتعلقة بالأمان.

تهدف هذه الأطروحة إلى تقديم نظرة شاملة وتقييم وتصنيف للحلول الحالية لنظام إدارة معلومات وأحداث الأمان (المعلومات الأمنية ونظام إدارة الأحداث)، مع التركيز على قدرتها على مواجهة التحديات الأمنية الحديثة والامتثال للمعايير التنظيمية. تهدف الدراسة إلى تسليط الضوء على نقاط القوة والحدود للحلول المختلفة لنظام إدارة معلومات وأحداث الأمان (المعلومات الأمنية ونظام إدارة الأحداث)، وكذلك الجوانب الأساسية التي تؤثر على فعاليتها، من خلال فحص معمق للوثائق والمنصات الموثوقة.

من خلال تسليط الضوء على هذه القضايا، تأمل الدراسة في مساعدة عملية اتخاذ القرار الواعية في اختيار أفضل حل لنظام إدارة معلومات وأحداث الأمان (المعلومات الأمنية ونظام إدارة الأحداث) لاحتياجات المنظمة المحددة. تهدف الأطروحة إلى تزويد أصحاب المصلحة بالمعرفة والرؤى اللازمة للتنقل بشكل صحيح في البيئة المعقدة لحلول الأمن السيبراني من خلال فحص شامل لوظائف ومزايا ومقاييس أداء نظام إدارة معلومات وأحداث الأمان (المعلومات الأمنية ونظام إدارة الأحداث).

أخيرًا، تهدف هذه الدراسة إلى المساهمة في المناقشة المستمرة حول الأمن السيبراني من خلال تقديم رؤى قيمة حول الدور المتطور لحلول نظام إدارة معلومات وأحداث الأمان (المعلومات الأمنية ونظام إدارة الأحداث) في حماية المنظمات من التهديدات الناشئة وضمان مرونة بنيتها التحتية الرقمية في عالم مترابط بشكل متزايد.

الكلمات المفتاحية : تكنولوجيا الإنترنت، التهديدات السيبرانية، تدابير الأمان، (المعلومات الأمنية ونظام إدارة الأحداث)، البنية التحتية لتكنولوجيا المعلومات، الامتثال التنظيمي، تحديات الأمان، سلامة البيانات، اتخاذ القرار، حلول الأمن السيبراني، مقاييس الأداء، أمن المعلومات، اكتشاف التهديدات، إدارة المخاطر