

الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 5491 - سيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbès



Graduation Thesis

To obtain the diploma of **Master's Degree**

Field of Study: **Computer Science**

Specialization: **Computer Systems Engineering (ISI)**

Theme

**A State-of-the-Art of SIEM-Based Cyber Attack
Detection Techniques.**

Presented by
CHERRAK Ismail Anis

Defended on: **June, 2026**
In front of the jury composed of

Dr. Nemdili Amel
Dr. Baba-Ahmed Manel
Dr. Naib Rabia

President of the Jury
Thesis Supervisor
Examiner

Academic Year: 2025/2026

Abstract

The rapid evolution of IT infrastructures and the growing sophistication of cyber threats have made centralized security monitoring an operational necessity for modern organizations. This thesis presents a comprehensive state-of-the-art study of Security Information and Event Management (SIEM) systems, with a particular focus on their role in cyber attack detection. The work begins by establishing the theoretical foundations of cybersecurity, covering threat taxonomies, attack methodologies, and the limitations of traditional defense mechanisms. It then reviews the generational evolution of SIEM platforms, from rule-based aggregation to AI-driven, cloud-native architectures, and surveys key research contributions in machine learning-based anomaly detection, User and Entity Behavior Analytics (UEBA), alert management, and SOAR integration. A structured comparative evaluation of six widely deployed SIEM solutions, Wazuh, Splunk Enterprise Security, FortiSIEM, Graylog, Elastic SIEM, and Exabeam, is conducted against 47 technical criteria spanning log collection, detection, automation, scalability, compliance, and cost. The results show that while no single platform achieves universal superiority, Elastic Security Enterprise offers the most complete feature coverage, while Exabeam and Graylog Enterprise lead in behavioral analytics and cost-effectiveness respectively. The study concludes by identifying persistent research gaps including false positive reduction at scale, model explainability, and privacy-preserving detection architectures.

Keywords: SIEM, Cyber Attack Detection, Machine Learning, Anomaly Detection, UEBA, SOAR, Threat Intelligence, Comparative Study, Cybersecurity

Résumé

L'évolution rapide des infrastructures informatiques et la sophistication croissante des cybermenaces ont fait de la supervision de sécurité centralisée une nécessité opérationnelle pour les organisations modernes. Ce mémoire présente une étude approfondie de l'état de l'art des systèmes de gestion des informations et des événements de sécurité (SIEM), avec un accent particulier sur leur rôle dans la détection des cyberattaques. Le travail débute par l'établissement des fondements théoriques de la cybersécurité, couvrant les taxonomies des menaces, les méthodologies d'attaque et les limites des mécanismes de défense traditionnels. Il passe ensuite en revue l'évolution générationnelle des plateformes SIEM, des architectures à base de règles jusqu'aux architectures cloud-native pilotées par l'intelligence artificielle, et recense les contributions de recherche clés en matière de détection d'anomalies par apprentissage automatique, d'analyse comportementale des utilisateurs et des entités (UEBA), de gestion des alertes et d'intégration SOAR. Une évaluation comparative structurée de six solutions SIEM largement déployées, Wazuh, Splunk Enterprise Security, FortiSIEM, Graylog, Elastic SIEM et Exabeam, est réalisée selon 47 critères techniques couvrant la collecte de journaux, la détection, l'automatisation, la scalabilité, la conformité et le coût. Les résultats montrent qu'aucune plateforme n'atteint une supériorité universelle, bien qu'Elastic Security Enterprise offre la couverture fonctionnelle la plus complète, tandis qu'Exabeam et Graylog Enterprise se distinguent respectivement en analytique comportementale et en rapport qualité-prix. L'étude conclut en identifiant des lacunes de recherche persistantes, notamment la réduction des faux positifs à grande échelle, l'explicabilité des modèles et les architectures de détection respectueuses de la vie privée.

Mots-clés : SIEM, Détection de cyberattaques, Apprentissage automatique, Détection d'anomalies, UEBA, SOAR, Renseignement sur les menaces, Étude comparative, Cybersécurité

ملخص

أدى التطور السريع للبنى التحتية المعلوماتية وتزايد تعقيد التهديدات السيبرانية إلى جعل مراقبة الأمن المركزية ضرورة تشغيلية للمؤسسات الحديثة. تقدم هذه المذكرة دراسة شاملة لحالة الفن في أنظمة إدارة معلومات وأحداث الأمن، (SIEM) مع التركيز على دورها في الكشف عن الهجمات السيبرانية. يبدأ العمل بإرساء الأسس النظرية للأمن السيبراني، إذ يتناول تصنيفات التهديدات ومنهجيات الهجوم وحدود آليات الدفاع التقليدية. ثم يستعرض التطور الجيلي لمنصات SIEM من الأنظمة القائمة على القواعد إلى البنى السحابية المدعومة بالذكاء الاصطناعي، ويرصد الإسهامات البحثية الرئيسية في مجال كشف الشذوذ بالتعلم الآلي، وتحليل سلوك المستخدمين والكيانات، (UEBA) وإدارة التنبهات، وتكامل SOAR. كما يُجري دراسة مقارنة منهجية لستة حلول SIEM واسعة الانتشار، Wazuh وEnterprise Splunk وSecurity Elastic وFortiSIEM وGraylog وSIEM Elastic وExabeam، وفق 47 معياراً تقنياً تشمل جمع السجلات والكشف والأتمتة وقابلية التوسع والامتثال التنظيمي والتكلفة. تُظهر النتائج أنه لا توجد منصة واحدة تحقق التفوق المطلق، غير أن Security Elastic وEnterprise تقدم أشمل تغطية وظيفية، في حين تتميز Exabeam وEnterprise Graylog بالتحليل السلوكي والفعالية من حيث التكلفة على التوالي. تختتم الدراسة بتحديد الثغرات البحثية القائمة، ولا سيما تقليص الإيجابيات الكاذبة على نطاق واسع، وقابلية تفسير النماذج، وبنى الكشف الصديقة للخصوصية.

الكلمات المفتاحية: SIEM، كشف الهجمات السيبرانية، التعلم الآلي، كشف الشذوذ، UEBA، SOAR، استخبارات التهديدات، دراسة مقارنة، الأمن السيبراني