AVIS DE SOUTENANCE D'UNE THESE DE DOCTORAT

Le Directeur de l'Ecole Nationale des Sciences Appliquées a le plaisir d'informer le public qu'une soutenance de thèse de Doctorat en

«Sciences et ingénierie»

aura lieu le 11/04/2026 à 12H00 l'ENSA, Kénitra

La Thèse sera présentée par Mr RADAH TAREK

Sous le thème :

Détection Avancée des Menaces et Automatisation Intelligente de la Réponse : Application de l'IA aux Centres d'Opérations de Sécurité

Devant le jury composé de :

Nom et Prénom	Titre	Etablissement
HACHIMI HANAE	Président	ENSA, Kénitra
ZELLOU AHMED	Rapporteur	ENSIAS
KORCHIYNE REDOUANE	Rapporteur	EST, Kénitra
DAHA BELGHITI IMANE	Rapporteur	EST, Salé
CHIHAB YOUNES	Examinateur	EST, Kénitra
AIT MADI ABDESSALAM	Examinateur	ENSA, Kénitra
SAADI CHAIMAE	Co-Directeur de thèse	EST, Kénitra
CHAOUI HABIBA	Directeur de thèse	ENSA, Kénitra

UNIVERSITE IBN TOFAIL ★ PÔLE DES ETUDES DOCTORALES ★ KENITRA

Université Ibn Tofail
جامعة ابن طفيل
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵉⴱⵏ ⵟⴼⴰⵢⵍ Ibn Tofail University

المملكة المغربية
وزارة التعليم العالي
والبحث العلمي والابتكار

Nom et Prénom : RADAH TAREK
Date de soutenance : 11/04/2026
Directeur de Thèse : CHAOUI HABIBA

Sujet de thèse :

Détection Avancée des Menaces et Automatisation Intelligente de la Réponse : Application de l'IA aux Centres d'Opérations de Sécurité

Résumé:

L'essor des technologies numériques a considérablement élargi la surface d'attaque des organisations, faisant de la cybersécurité un enjeu majeur de résilience économique et de souveraineté nationale. Les cadres de référence internationaux (NIST, ISO/IEC 27001) et le modèle MITRE ATT&CK démontrent que les mécanismes de prévention seuls sont insuffisants, rendant la détection et la réponse indispensables pour limiter l'impact des cyberattaques. La pratique de la détection demeure un domaine à forte complexité scientifique, nécessitant une synergie disciplinaire : science des données, ingénierie logicielle, connaissance des menaces et pratiques opérationnelles de sécurité. Le processus repose sur trois phases : collecte de données et de télémétrie, analyse et corrélation des événements, et remédiation fondée sur l'output analytique. Chaque étape soulève des défis persistants : volumes massifs de données, taux élevés de faux positifs, manque de contextualisation des alertes, et difficultés d'automatisation de la réponse. L'intelligence artificielle et l'apprentissage automatique offrent des pistes prometteuses pour renforcer les capacités des SOC, malgré des défis liés à la qualité des données et à l'intégration opérationnelle.

Cette thèse traite les défis opérationnels des centres d'opérations de sécurité (SOC) comme des problèmes fondamentalement liés aux données, mobilisant les avancées récentes en IA et science des données pour apporter des solutions innovantes. Elle démontre comment ces avancées permettent de dépasser les limites des approches traditionnelles de détection et d'automatisation de la réponse. Composée de six chapitres, elle présente des contributions scientifiques couvrant le cycle complet de la détection et réponse aux incidents, de la collecte à la confidentialité.

Mots Clés :SOC, Réponse aux incidents, Cybersécurité,IA, LLM, Malware, SIEM, Automatisation

Abstract:

The rise of digital technologies has significantly expanded organizations' attack surface, making cybersecurity a major issue for economic resilience and national sovereignty. International reference frameworks (NIST, ISO/IEC 27001) and the MITRE ATT&CK model demonstrate that prevention mechanisms alone are insufficient, making detection and response essential to limit cyberattack impact.Detection practice remains a domain of high scientific complexity, requiring synergy across disciplines: data science, software engineering, threat intelligence, and operational security practices. The process relies on three main phases: (1) data and telemetry collection, (2) event analysis and correlation, and (3) remediation based on analytical output. Each step raises persistent challenges: massive data volumes, high false positive rates, lack of alert contextualization, and difficulties in response automation.Artificial intelligence and machine learning offer promising avenues to strengthen SOC capabilities, despite challenges related to data quality and operational integration.

This thesis addresses the operational challenges of Security Operations Centers (SOCs) as fundamentally data-driven problems, leveraging recent advances in AI and data science to provide innovative solutions. It demonstrates how these advances enable overcoming the limitations of traditional detection and response automation approaches in modern SOCs. Comprising six chapters, it presents scientific contributions that mitigate incident detection and response challenges, covering the complete cycle from data collection to privacy preservation.

Key words:SOC, Incident response, Cybersecurity, AI, LLM, Malware, SIEM, Automation