الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للاعلام الالي -8 ماي 1945- بسيدي بلعباس
École Supérieure en Informatique
-8 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **Master**
Field : **Computer Science**
Specialty : **Computer Systems Engineering**

Theme

Proactive Cybersecurity : An Overview of Cyber Threat Hunting

---

Presented by :
Nedjaa Ines

Defending on : **21 September 2025**
In front of the jury composed of

Dr. SOUYAH Amina	|	President
Dr. KHALDI Miloud	|	Supervisor
Dr. BENDELLA Mohammed Salih	|	Examinator

Academic Year : 2025-2026

Abstract

In today's increasingly interconnected world, cyber threats are evolving rapidly in both complexity and frequency. This constant evolution has made traditional, reactive cybersecurity approaches insufficient to provide adequate protection for organizations. While firewalls, intrusion detection systems, and antivirus solutions still play an important role, they are often unable to detect sophisticated, stealthy attacks that bypass automated defenses. As a result, organizations are facing the urgent need to adopt more efficient and proactive security strategies to defend their digital assets and maintain business continuity.

Cyber threat hunting (CTH) has emerged as a powerful and proactive approach to address this challenge. Instead of waiting for alerts or relying solely on automated tools, cyber threat hunting involves skilled analysts actively searching for hidden threats, indicators of compromise (IOCs), and suspicious behaviors inside organizational networks. This approach uses threat intelligence, data analytics, and hypothesis-driven investigations to identify attacks that may go unnoticed by conventional methods.

Our study focuses on cyber threat hunting and its key aspects, providing a comprehensive exploration of its methodologies, tools, challenges, and benefits. By highlighting the role of CTH in strengthening an organization's security posture, this research emphasizes the critical need for a proactive mindset and the integration of hunting practices within modern Security Operations Centers (SOCs).

Keywords : Cyber Threat Hunting (CTH), Proactive Security, Threat Intelligence, Indicators of Compromise (IOCs), Security Operations Center (SOC), Cyber Threats, Data Analytics, Hypothesis-Driven Investigations, Stealthy Attacks.

Résumé

Dans un monde où tout est de plus en plus connecté, les cybermenaces évoluent rapidement, devenant plus complexes et plus fréquentes. Face à cette évolution constante, les approches traditionnelles et réactives en cybersécurité ne suffisent plus à protéger efficacement les organisations. Bien que les outils comme les pare-feux, les systèmes de détection d'intrusion ou les antivirus soient encore utiles, ils peinent souvent à repérer les attaques sophistiquées et discrètes qui échappent aux défenses automatisées. Les organisations doivent donc adopter de nouvelles stratégies plus efficaces et surtout proactives pour protéger leurs ressources numériques et assurer la continuité de leurs activités.

La chasse aux menaces s'impose comme une réponse innovante à ce défi. Contrairement aux approches classiques qui attendent qu'une alerte se déclenche, cette pratique consiste à mener des recherches actives pour détecter les menaces cachées et les comportements suspects dans les réseaux informatiques. Elle s'appuie sur l'expertise des analystes, l'intelligence sur les menaces, l'analyse des données et des enquêtes guidées par des hypothèses pour identifier les attaques qui passeraient inaperçues autrement.

Notre étude explore la chasse aux menaces et ses principaux aspects, en analysant ses méthodes, ses outils, ses défis et ses apports. Elle met en avant l'importance d'adopter une démarche proactive et d'intégrer ces pratiques au sein des Centres d'opérations de sécurité modernes pour renforcer la posture globale de sécurité des organisations.

Mots clés : Cybermenaces, Démarche proactive, Chasse aux menaces, Intelligence sur les menaces, Analyse des données, Centres d'opérations de sécurité.

ملخص

في عالمنا المعاصر المترابط، تتطور التهديدات السيبرانية بسرعة كبيرة، وتزداد تعقيدًا وتكرارًا يومًا بعد يوم. هذا التطور جعل الأساليب التقليدية القائمة على ردّ الفعل غير كافية لحماية المؤسسات بالشكل المطلوب. فرغم أهمية أنظمة كشف التسلل وبرامج مكافحة الفيروسات، إلا أنها غالبًا تعجز عن اكتشاف الهجمات المعقدة والمخفية التي تتجاوز الدفاعات الآلية. لذلك، باتت المؤسسات بحاجة ماسة إلى تبني استراتيجيات أكثر كفاءة واستباقية لحماية أصولها الرقمية وضمان استمرار أعمالها.

يُعتبر صيد التهديدات السيبرانية أحد أبرز الحلول الحديثة لهذه المشكلة، إذ يعتمد على البحث النشط والمبادر عن التهديدات الخفية والسلوكيات المشبوهة داخل الشبكات، بدلاً من انتظار وصول التنبيهات. يقوم بهذه المهمة محللون ذو خبرة، مستخدمين معلومات استخباراتية وتحليل البيانات، وتحقيقات قائمة على الفرضيات، بهدف اكتشاف الهجمات التي قد لا تلتقطها الأنظمة التقليدية.

تركز دراستنا على صيد التهديدات السيبرانية من خلال تسليط الضوء على أهم جوانبه، بما في ذلك المنهجيات، الأدوات، التحديات والفوائد. كما تؤكد الدراسة على أهمية تبني عقلية استباقية ودمج هذه الممارسات ضمن مراكز العمليات الأمنية الحديثة لتعزيز القدرة الدفاعية للمؤسسات.

الكلمات المفتاحية : صيد التهديدات السيبرانية، التهديدات السيبرانية، تحليل البيانات، مركز عمليات الأمن.