Kingdom Of Saudi Arabia
Ministry Of Education
Onaizah Colleges
College of Engineering and IT
Computer Science Department
Cyber Security Program

المملكة العربية السعودية
وزارة التعليم
كليات عنيزة الأهلية
كلية الهندسة وتقنية المعلومات
قسم علوم الحاسب
برنامج الأمن السيبراني

**RESEARCH PROPOSAL TITLE**

# The Role of Threat Intelligence in Modern Cybersecurity

**Course** Name: Introduction to Cyber Security and Digital Crimes
**Course Code:** CYS 111
**Student Name: Mayar Yousef Alsaeed**
**ID No.: 461210731**

# 1. Introduction

In today's digital world, cyber threats are increasing rapidly and becoming more complex. Organizations, governments, and individuals are facing different types of cyberattacks such as phishing, ransomware, and data breaches [1]. To defend against these threats, cybersecurity experts rely on Threat Intelligence (TI) — the process of collecting, analyzing, and using information about potential and existing cyber threats [2].

The role of threat intelligence is to help organizations understand the attacker's goals, techniques, and tools, so they can take the right actions to prevent or reduce attacks before they happen.

## 2. Background and statement of the problem

In the past, cybersecurity focused mainly on using firewalls, antivirus software, and encryption [3]. However, these traditional tools are not enough against modern, advanced attacks. Many organizations were reacting to threats *after* they happened, which caused financial and data losses [4].

The main problem is that cybercriminals are using advanced methods such as social engineering, AI-powered attacks, and zero-day vulnerabilities [5]. Without understanding these threats in advance, organizations remain vulnerable. Threat intelligence fills this gap by providing early warning and actionable data. It allows security teams to be proactive instead of reactive.

## 3. Research aim and objectives

The aim of this research is to explain the importance of threat intelligence in modern cybersecurity and how it improves the protection of digital systems.

The main objectives are:

1. To define what threat intelligence means in cybersecurity.
2. To describe the types and sources of threat intelligence.
3. To discuss how organizations use threat intelligence to defend against cyber threats.
4. To highlight the benefits and challenges of implementing threat intelligence.

## 4. Results and Discussion

### 1. Definition and Types of Threat Intelligence

Threat intelligence is information that helps identify, understand, and respond to cyber threats [1]. It can be divided into three main types:

- **Strategic Threat Intelligence:** High-level information about global threats, used by managers and decision-makers.

- **Tactical Threat Intelligence:** Focuses on the techniques and tools used by attackers, helping security teams build better defense systems[2].
- **Operational Threat Intelligence:** Provides real-time data about ongoing attacks, such as IP addresses or malware signatures [3].

**2. Sources of Threat Intelligence**

Organizations collect intelligence from various sources such as:

- Security logs and monitoring systems [4].
- Open-source intelligence (OSINT) from public reports and websites [5].
- Dark web monitoring for stolen data or hacker activities [2].
- Information sharing between organizations and security communities [3].

**3. Benefits of Threat Intelligence**

Threat intelligence helps organizations detect and stop attacks earlier. It improves incident response, reduces damage, and saves time [1].

It also supports decision-making by identifying which assets are most at risk and where to focus defenses[4].

For example, financial institutions use threat intelligence to track phishing campaigns targeting their customers, and governments use it to protect national infrastructure from cyber espionage and terrorism[5].

**4. Challenges in Threat Intelligence**

Despite its benefits, there are some challenges. Collecting large amounts of data can be expensive and time-consuming. Sometimes, intelligence information can be outdated or inaccurate [3].

Also, small organizations may lack experts or tools to analyze the data properly. Therefore, successful use of threat intelligence requires skilled analysts and strong cooperation between different teams.

## 5. Conclusion:

Threat intelligence plays a critical role in modern cybersecurity. It transforms the security approach from reactive to proactive, allowing organizations to predict and prevent cyberattacks more effectively [2].

By understanding who the attackers are, what their motives are, and how they operate, organizations can strengthen their defense systems and reduce cyber risks.

Although there are challenges, the advantages of using threat intelligence clearly outweigh the difficulties. Continuous investment in threat intelligence will remain essential for protecting digital environments in the future [5].

# 6. References:

[1] R. M. Lee, M. Assante, and T. Conway, “The Industrial Control System Cyber Kill Chain,” *SANS Institute*, 2015.

[2] FireEye, “What is Cyber Threat Intelligence,” *FireEye.com*, 2021.

[3] IBM Security, “The Importance of Threat Intelligence in Cybersecurity,” *IBM*, 2022.

[4] Palo Alto Networks, “Types of Cyber Threat Intelligence,” *Paloaltonetworks.com*, 2023.

[5] Trend Micro, “Understanding Threat Intelligence and Its Benefits,” *Trendmicro.com*, 2023.