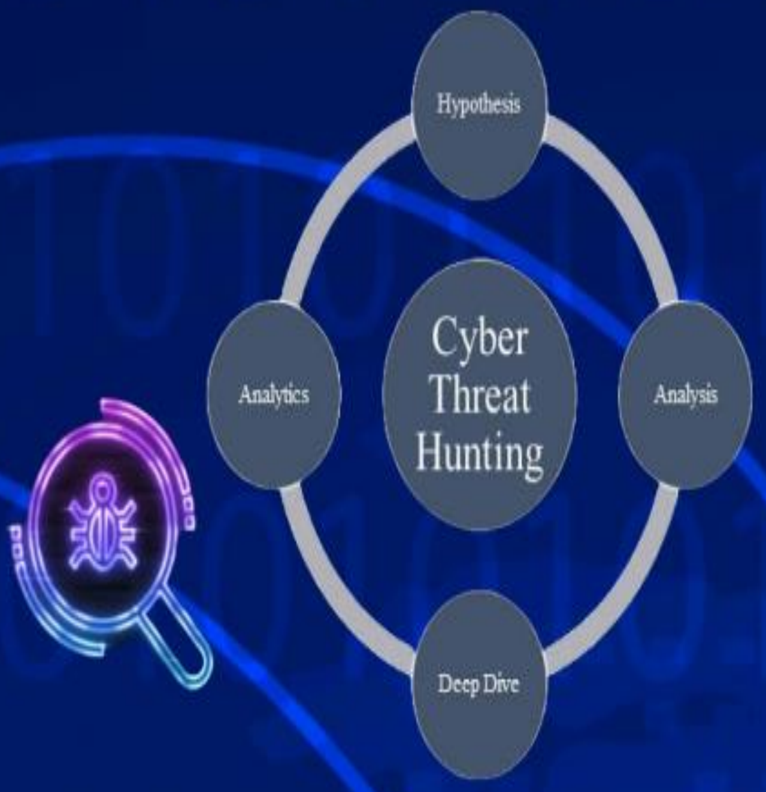
MSc in Cybersecurity, Privacy and Trust

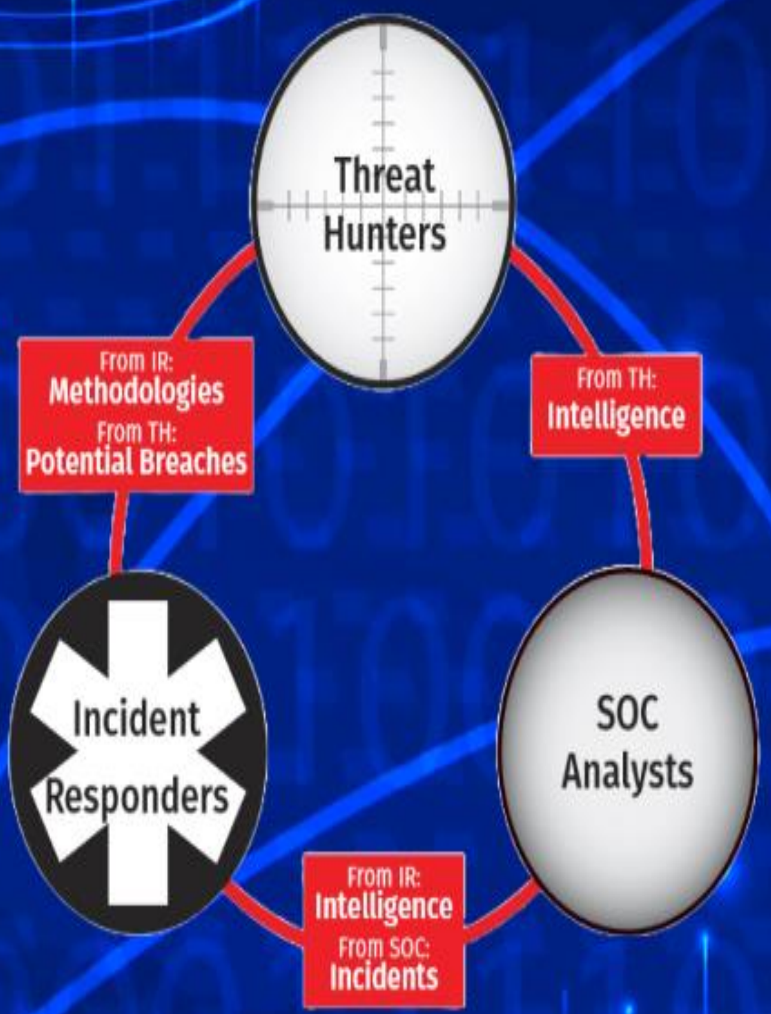
How to implement Threat Hunting in small to medium-sized enterprises

Student: Rizo Jusufovic, C00292061@setu.ie, Supervisor: Paul Barry, paul.barry@setu.ie

I. Introduction: What is Threat Hunting?

"Put you in the Mindset of the Hacker, you act as advisory - hacker hunter"





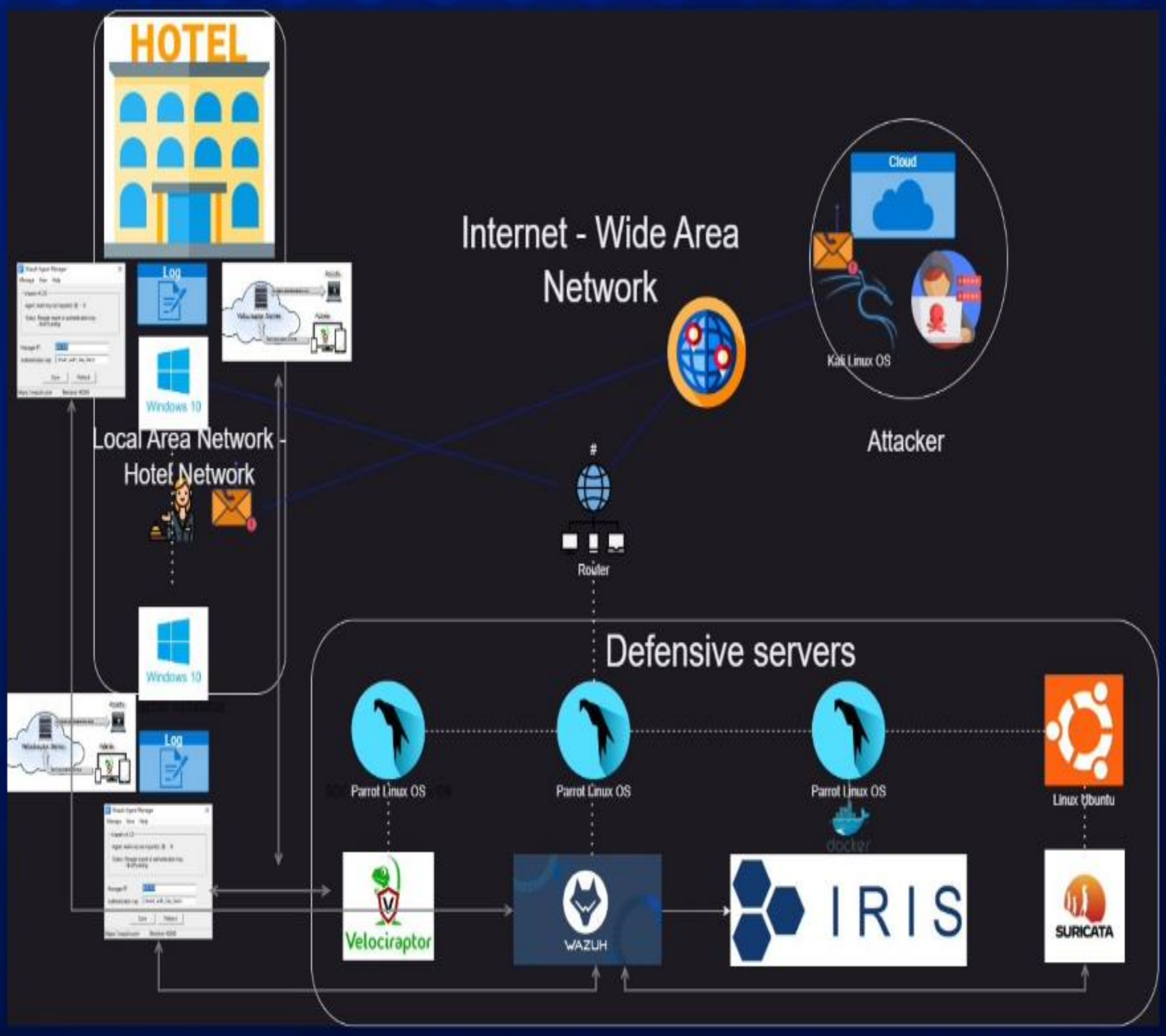
II. Research Questions:

Research explores various techniques for threat hunting:

1. Hypothesis-driven hunting
2. Indicator of Compromise (IOC) hunting
3. Machine learning and analytics-driven hunting
4. Threat intelligence-driven hunting

III. Literature Review:

Threat hunting involves a "Proactive Approach" and the search for cyber threats that may be silently lurking within a network, escaping conventional detection. The objective of threat hunting is to uncover novel techniques, tactics, and procedures (TTPs), enabling the anticipation of emerging threats (Ajmal et al., 2021).



IV. Research Methodology:

The research methodology adopts an exploratory approach to investigate the implementation of threat hunting techniques within the context of SMEs specifically focusing on the hotel industry.

The study aims to assess the effectiveness of four distinct threat hunting methodologies within the hotel network environment.

V. Technologies:

Open Source Tools:

Wazuh - SIEM

Velociraptor - Advanced Incident Response

Suricata -NDS/IDS

DFIR-Iris - Collaborative Platform

Linux Kali - Offensive OS

Linux Parrot - Defensive OS