MALLA REDDY UNIVERSITY
(As per Telangana State Private Universities Act No.11 of 2018 and G.O.Ms.No.14, Higher Education (UE) Department)

Unified Cyber Threat Detection and Incident Management System

ABSTRACT

The **Unified Cyber Threat Detection and Incident Management System** is a comprehensive cybersecurity solution designed to enhance an organization's security posture using Wazuh SIEM for real-time threat detection, analysis, and response. Acting as a centralized security monitoring system, it collects and analyzes log and event data from various sources, including network devices, endpoints, cloud environments, and applications. As cyber threats become more advanced, organizations require proactive security measures to detect and stop attacks before they cause harm. This system leverages machine learning, correlation rules, and threat intelligence to identify suspicious activities, investigate incidents, and automate responses, significantly reducing security risks. Deployed within a Security Operations Center (SOC), it enables security teams to continuously monitor threats, detect vulnerabilities, and respond swiftly to potential cyberattacks. Its automated incident response mechanisms ensure rapid containment of security breaches, minimizing damage, downtime, and operational disruptions. The system also helps organizations comply with industry regulations and security standards. With real-time security insights, forensic investigation tools, and compliance reporting, it strengthens an organization's ability to prevent, detect, and respond to cyber threats effectively. This powerful solution bridges the gap between threat detection, incident response, and compliance management, making it an indispensable component of modern cyber defense strategies.

SI.NO	Roll No	Name	Signature of the student
1	2111CS040005	P. ADITYA SRIRAM	

Date of Submission: **Name &Signature of the Guide:**

Dr. G Anand Kumar