

# HCA-Guard: Human & Configuration Analysis Guard

Sree Vishnu H<sup>1</sup>

<sup>1</sup>B.Sc Digital & Cyber Forensics Science,  
Rathinam College of Arts and Science, Coimbatore - 641021, India.

\*\*\*

**Abstract** - The rapid expansion of digital systems has significantly increased exposure to cybersecurity threats. While modern security tools are capable of detecting known attack patterns, many real-world compromises still occur due to weak system configurations and improper user management. These issues are often simple but can lead to serious security incidents if not addressed proactively. This paper presents HCA-Guard (Human & Configuration Analysis Guard), a host-based intrusion detection and response system designed to address these practical challenges. The system focuses on analyzing system configurations, user privileges, and service exposure to identify potential vulnerabilities. It incorporates key features such as reverse shell detection, risk scoring, and automated response mechanisms to improve threat mitigation. When suspicious activity is detected, the system evaluates its severity and performs appropriate actions such as process termination and alert generation. The system operates entirely at the host level, ensuring data privacy and reducing dependency on external infrastructure. Experimental evaluation under different scan modes shows that HCA-Guard can effectively identify both minor misconfigurations and critical vulnerabilities with minimal performance overhead. The results demonstrate that focusing on configuration and human-related risks provides a practical and effective approach to improving endpoint security.

**Key Words:** Cyber Security, Intrusion Detection, Configuration Analysis, Human Risk Assessment, Reverse Shell Detection, Endpoint Security, Digital Forensics

## 1. INTRODUCTION

The increasing reliance on digital systems in everyday life has made cybersecurity a fundamental requirement rather than an optional feature. From personal devices to enterprise-level infrastructures, systems are continuously exposed to threats that target confidentiality, integrity, and availability, and as technology advances, the attack surface also expands, making it easier for attackers to exploit vulnerabilities. Although significant progress has been made in developing security tools, many existing solutions primarily focus on detecting known attack signatures or patterns, which, while effective against previously identified threats, do not fully address the dynamic nature of modern cyber-attacks. In many practical situations, attackers exploit simple weaknesses such as poorly configured systems, weak authentication mechanisms, and improper user privilege management. It is commonly observed that security breaches occur due to issues such as misconfigured system settings, unnecessary service exposure, excessive user privileges, and lack of continuous monitoring, and these factors are often underestimated because they do not appear as direct threats, yet they significantly increase the risk of system compromise. To address these challenges, this paper introduces HCA-Guard, a host-based intrusion detection and response system that focuses on both configuration analysis and human-related risk factors, aiming to identify internal weaknesses, evaluate risk levels, and provide appropriate response mechanisms, thereby offering a practical and effective approach to improving system security.

## 2. LIMITATIONS OF EXISTING SYSTEM

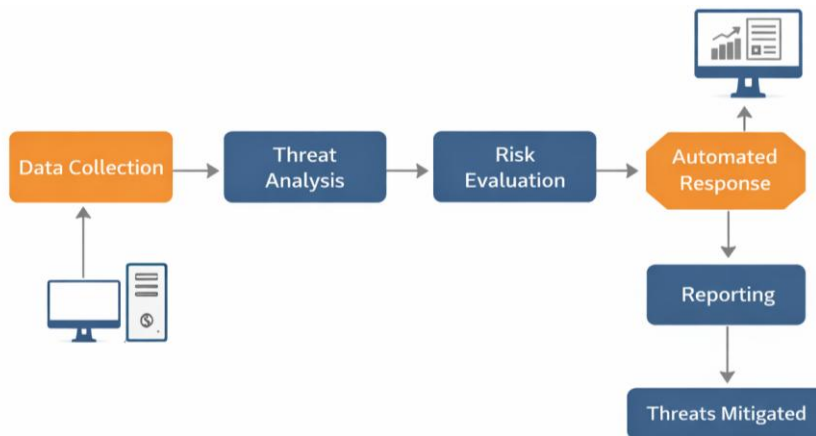
Despite the availability of numerous cybersecurity tools and frameworks, several practical limitations continue to affect their effectiveness in real-world environments. One of the primary limitations is the heavy reliance on signature-based detection techniques, which are effective in identifying known threats but fail to detect new, unknown, or modified attack patterns, allowing emerging threats to bypass traditional security mechanisms. Another key limitation is the lack of proper configuration-level analysis, as many systems do not actively verify whether a system is securely configured, leaving issues such as open ports, unnecessary services, and weak or misconfigured security policies undetected, thereby increasing the attack surface. Human-related risks are also frequently overlooked, where users may have excessive privileges, follow weak authentication practices, or manage accounts improperly, unintentionally introducing serious vulnerabilities that are not adequately addressed by traditional security solutions. Furthermore, many modern systems depend on cloud-based infrastructures, which introduce concerns related to privacy, latency, and system dependency, making them unsuitable for certain environments. Another major challenge is the generation of excessive alerts without proper prioritization, leading to alert fatigue and making it difficult for users to identify critical threats. These limitations highlight the need for a more practical

approach that focuses not only on threat detection but also on identifying and mitigating configuration and human-related risk factors within the system.

**Table -1: Scan Results of HCA-Guard**

Scan Mode	Description	Observation
Basic Scan	Performs initial system checks	Minor issues detected
Medium Scan	Includes configuration analysis	Moderate risks identified
Deep Scan	Full system evaluation	Critical vulnerabilities found

The results presented in Table 1 demonstrate the effectiveness of HCA-Guard across different scan modes. The Basic Scan identifies minor issues, while the Medium Scan detects moderate risks related to system configuration. The Deep Scan performs a comprehensive evaluation and successfully identifies critical vulnerabilities. These observations indicate that the system can detect and categorize risks based on severity, enabling efficient prioritization and improving overall system security.



**Fig -1: System Architecture of HCA-Guard**

The system architecture of HCA-Guard illustrates the complete workflow of the proposed intrusion detection and response system. The process begins with data collection from the host system, including system configurations, user activities, and running processes. This data is then passed to the analysis module, where potential threats and anomalies are identified. The risk evaluation component assesses the severity of detected issues based on predefined criteria and assigns appropriate risk levels. Based on the evaluated risk, the system triggers automated response mechanisms such as process termination or alert generation. Finally, the reporting module provides a clear summary of detected vulnerabilities and actions taken, enabling users to understand and improve the security posture of the system.

### 3. PROPOSED SYSTEM

The proposed system, HCA-Guard, is designed as a host-based intrusion detection and response framework that focuses on identifying both configuration-related vulnerabilities and human-centric risks. The system continuously monitors system configurations, user privileges, and running processes to detect anomalies and potential threats. It integrates modules such as data collection, threat analysis, risk evaluation, automated response, and reporting to ensure effective threat detection and

mitigation. By operating at the host level, the system maintains data privacy and reduces dependency on external infrastructures while providing efficient and real-time security analysis.

#### **4. METHODOLOGY**

The methodology of HCA-Guard follows a structured approach consisting of data collection, analysis, and response. Initially, the system gathers host-level data including system configurations, user privileges, and active processes, which are then analyzed to identify anomalies, misconfigurations, and potential security vulnerabilities. A risk scoring mechanism is applied to classify detected issues based on their severity levels, and based on the evaluated risk, appropriate actions are triggered through the automated response module, such as alert generation or process termination. The system operates with continuous monitoring and periodic scanning to ensure consistent security and system stability.

#### **5. RESULTS AND ANALYSIS**

The system performance remained stable across different scan modes without significant resource overhead. The Basic Scan mode was able to detect minor issues, while the Medium Scan identified moderate risks related to system configuration and policy settings. The Deep Scan mode provided a comprehensive evaluation and successfully detected critical vulnerabilities that could potentially compromise system security. The results indicate that HCA-Guard is capable of identifying both low-level misconfigurations and high-risk vulnerabilities effectively, and its ability to categorize risks based on severity allows users to prioritize actions and respond efficiently. Additionally, the automated response mechanism reduces the time required to handle threats, improving overall system security and reliability. The observed results confirm that the system performs efficiently with minimal overhead while maintaining effective threat detection capabilities.

#### **6. CONCLUSION**

This paper presented HCA-Guard, a host-based intrusion detection and response system designed to address practical cybersecurity challenges associated with system misconfigurations and human-related risks. Unlike traditional security solutions that primarily focus on signature-based detection, the proposed system emphasizes identifying underlying vulnerabilities that often lead to real-world security breaches. The results demonstrate that HCA-Guard is capable of effectively detecting and categorizing risks across different scan modes while maintaining system stability and low resource overhead, and the integration of automated response mechanisms further enhances the system's ability to mitigate threats in real time, reducing dependency on manual intervention. Overall, the proposed system provides a practical and efficient approach to improving endpoint security by combining configuration analysis, risk evaluation, and automated response, and future work may focus on enhancing detection accuracy through intelligent analysis techniques and extending the system to support network-level monitoring for broader security coverage.

#### **ACKNOWLEDGEMENT**

The author would like to express sincere gratitude to Dr. T. Velumani, Head of the Department, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, for his valuable guidance, support, and encouragement throughout the development of this work.

#### **REFERENCES**

- [1] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2018.
- [2] Center for Internet Security (CIS), "CIS Critical Security Controls," Version 8, 2021.
- [3] OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021.
- [4] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson, 2018.
- [5] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2003.

## BIOGRAPHIES



**Sree Vishnu H** is currently a B.Sc. Digital and Cyber Forensics Science student from Rathinam College of Arts and Science, Coimbatore, India. His interests include cybersecurity, penetration testing, and digital forensics.