Hive Sentinel:
The Hacker's Confine

Introduction

The "Hive Sentinel" project manages honeypots to enhance cybersecurity, diverting attackers and providing vital threat insights. Inspired by Deception 2.0 strategies, it offers:

- Automated deployment of honeypots
- Continuous monitoring
- Real-time threat detection
- Snapshot restoration
- MITRE ATT&CK framework mapping

Problem Statement

In collaboration with Cydea Tech, the company addresses the issue of the lack of a dedicated health monitoring system for honeypots. This absence can lead to risks such as a false sense of security and limited threat intelligence, leaving critical assets vulnerable to exploitation. Compromised honeypots can then serve as entry points for attackers to infiltrate networks, endangering other systems.

Motivation

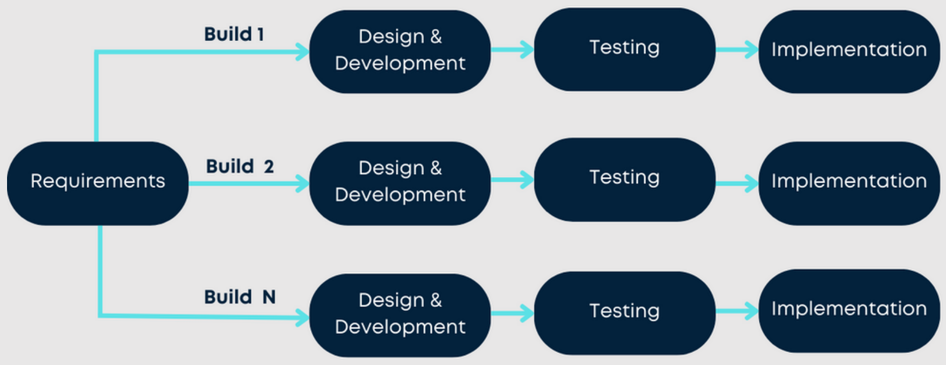
Protecting digital ecosystems demands vigilant oversight. Health monitoring of honeypots, in collaboration with Cydea Tech, ensures proactive threat detection and response, safeguarding networks from malicious actors. With comprehensive health monitoring and machine re-spawning capabilities, our goal is to forge a robust and resilient deception platform, enhancing protection against evolving threats.

Product Commercialization

Leveraging the expertise of Cydea Tech's specialists, our honeypot commercialization strategy prioritizes strategic deployment, user protection, and adaptability. This innovation fortifies organizational security, mitigating cyber risks and safeguarding critical data. Ultimately, it enhances personal information security, fostering a safer digital landscape for all.

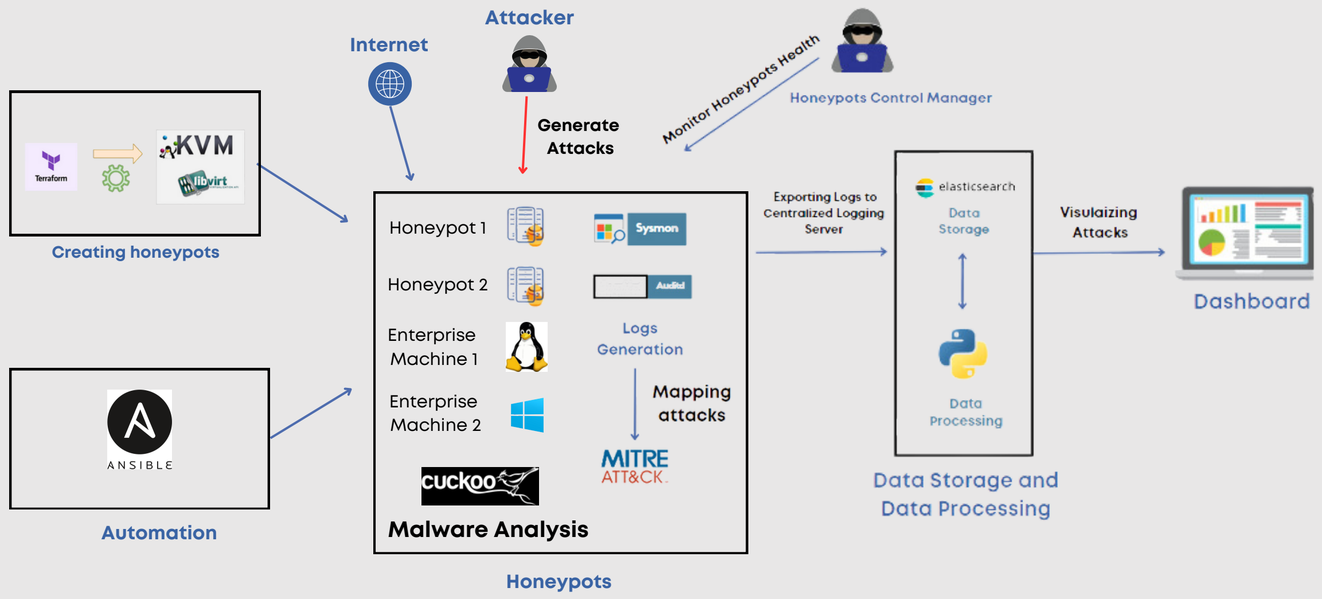
Methodology

The Hive Sentinel project embraces incremental methodology for steady progress and adaptability, breaking tasks into manageable chunks. Each iteration adds value, fostering continuous improvement and flexibility in response to changing requirements, moving steadily towards its ultimate goal.



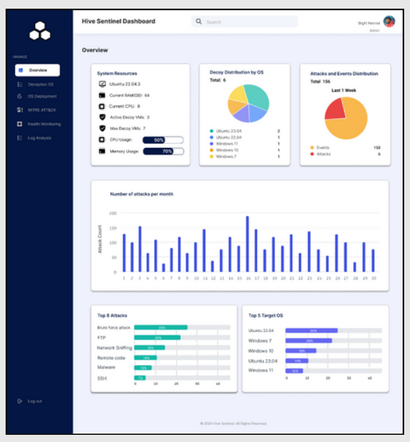
Architecture

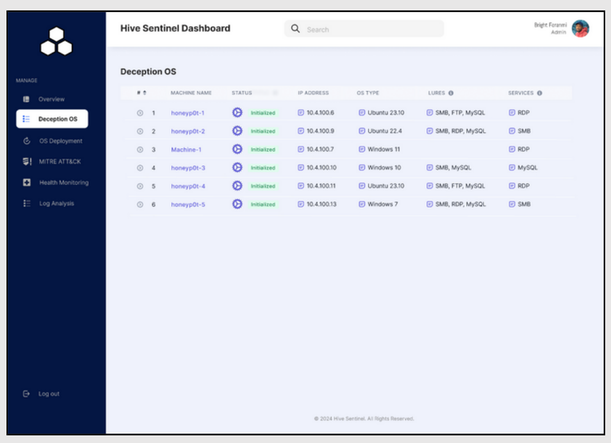
To efficiently execute the process of creating Hive Sentinel, a robust combination of frameworks and tools is essential. Architecture diagram presents the actions and activities that are necessary for achieving an effective deployment of a honeypot system. This integrated approach ensures a comprehensive cybersecurity framework, seamlessly combining virtualization, automation, monitoring, database management, security integration, and visualization, thereby ensuring an efficient honeypot system.

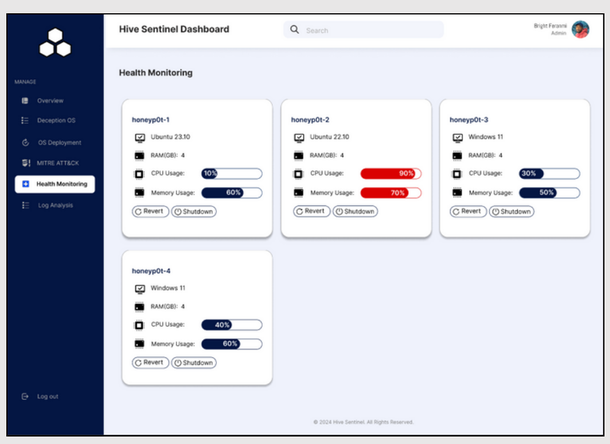


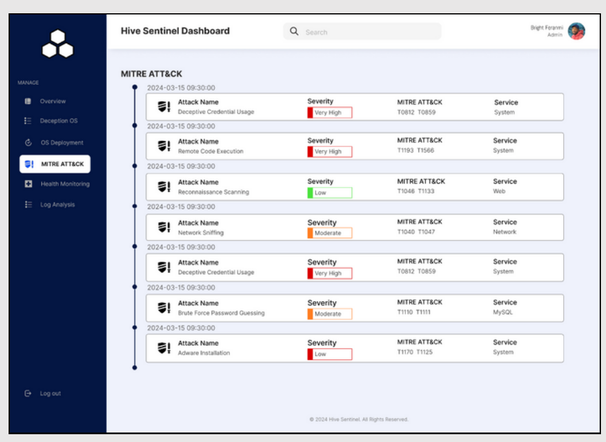
Expected Outcomes

Under the guidance and supervision of Dr. Nabeel Ahmed and Dr. Abdul Waheed khan, Project Hive Sentinel will be able to automate the deployment of high interaction honeypots for the deception platform 2.0. It will provide health monitoring, facilitate machine re-spawning, enable intelligence gathering from hackers, and present gathered information through visual dashboards for enhanced cybersecurity measures.









A project By

Collaborating Industry

Under the Supervision of

Mariyam & Qaseem Ul Hassan

Cydea Tech

Dr. Abdul Waheed Khan

School of Computing Sciences