**Project Design Phase-II**

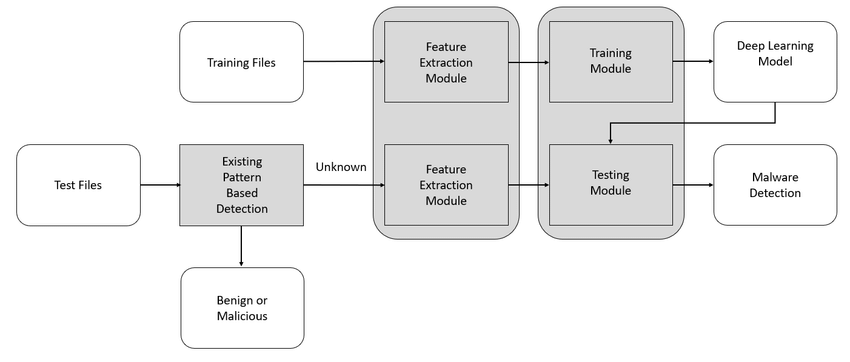
**Technology Stack (Architecture & Stack)**

|  |  |
| --- | --- |
| Date | 26 October 2022 |
| Team ID | 2.10 |
| Project Name | Project – Malware Detection & Classification |
| Maximum Marks | 4 Marks |

**Technical Architecture:**

The Deliverable shall include the architectural diagram as below and the information as per the table1 & table 2

**Example:**



**Table-1 : Components & Technologies:**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Component** | **Description** | **Technology** |
| 1. | User Interface | Enabling users to configure and customize detection rules and settings. | Configuration and Management. |
| 2. | incident Response Integration: | implementing automated actions or scripts to respond to threats. | Automated Response |
| 3. | Network Traffic Analysis | Examining network packets for signs of malicious activity. | Packet Capture and Analysis |
| 4. | Data Preprocessing: | Ensuring that data from different sources is transformed into a consistent format for analysis. | Data Normalization |
| 5. | Data Storage: | Storing logs, metadata, and threat intelligence data for historical analysis. | Database Systems |
| 6. | Machine Learning and AI: | Identifying relevant features from the data for machine learning models. | Feature Extraction |
| 7. | Behavior-Based Detection: | Rules and algorithms that flag suspicious behaviors. | Heuristics |
| 8. | APIs and Integrations: | APIs and connectors to interact with other security tools and platforms. | Integration Points |
| 9. | Data Collection and Acquisition: | Tools like Wireshark for capturing and analyzing network traffic. | Packet Capture Tools: |
| 10. | Access Control and Security: | Ensuring secure access to the system and its data. | Authentication and Authorization |
| 11. | Compliance and Reporting: | Ensuring the system adheres to relevant industry and regulatory standards. | Compliance Tools |

**Table-2: Application Characteristics:**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Characteristics** | **Description** | **Technology** |
| 1. | Real-Time Monitoring | Malware detection systems continuously monitor network traffic, files, and system activities in real-time to identify and respond to threats as they occur. | Heuristic Analysis, Signature-Based Detection |
| 2. | Anomaly Detection | Malware detection systems can identify deviations from normal network and system behavior, which may indicate a compromise. | Graph Analytics, Flow Analysis, Clustering and Segmentation |
| 3. | Incident Response Integration | Integration with incident response systems and workflows to facilitate a coordinated response to security incidents. | Security Information and Event Management (SIEM) Systems |
|  |  |  |  |
| 4. | Multilayered Approach | They employ multiple detection techniques, including signature-based, behavior-based, and heuristics-based methods, to detect a wide range of malware. | Security Information and Event Management (SIEM) Systems, Intrusion Detection and Prevention Systems (IDS/IPS |
| 5. | Scalability | Effective malware detection systems can scale to accommodate the growing volume of data and traffic in a network or organization. | Distributed Architecture, Scalable Network Traffic Analysis: |