ROAD MAP FOR THE SECURITY PROJECT #02

PHASE 1: PROJECT SETUP & REQUIREMENTS (24 SEP – 8 OCT)

1. **24 Sep:**
   - **Initial Setup:**
     - Install and configure the Wazuh and ELK stack (Elasticsearch, Logstash, Kibana).
     - Set up the basic environment for real-time data collection and monitoring.
     - Ensure all required dependencies and software components are installed.
2. **8 Oct:**
   - **Requirements Gathering & Use Case Definition:**
     - Define the key use cases (Anomalous File Creation, Suspicious Logins, etc.).
     - Document technical requirements for data ingestion and machine learning algorithms.
     - Collect sample data and logs for anomaly detection.

PHASE 2: DATA COLLECTION & PROCESSING (8 OCT – 22 OCT)

3. **22 Oct:**
   - **Data Collection Mechanism:**
     - Integrate Wazuh agents with various endpoints (servers, network devices).
     - Configure Logstash to collect and process logs from various sources (file systems, network, registry, etc.).
     - Set up File Integrity Monitoring (FIM) and Intrusion Detection System (IDS) rules in Wazuh.
     - Ensure logs are centralized in Elasticsearch and visualized in Kibana.
     - Start with key log sources: user logins, network activity, and file creation events.

Phase 3: Machine Learning Integration (22 Oct – 19 Nov)

4. **5 Nov:**
    - **Initial ML Model Development:**
        - Identify relevant Machine Learning algorithms (e.g., Isolation Forest, Autoencoders, or K-Means Clustering) for anomaly detection.
        - Develop initial ML models and train them using historical log data.
        - Define normal behavior patterns for each use case (e.g., logins, network activity, file creation) and identify deviations.

5. **19 Nov:**
    - **Model Training and Testing:**
        - Test the models on different use cases:
            - Anomalous File Creation.
            - Suspicious volume of logins (by user, by type).
            - Anomalous SMB connections.
            - Symbolic Link to Shadow Copy creation.
        - Fine-tune the ML models for better accuracy and performance.
        - Begin real-time anomaly detection and visualization in Kibana.

Phase 4: Real-Time Alerts & Visualization (19 Nov – 3 Dec)

6. **3 Dec:**
    - **Alerting and Visualization:**
        - Implement real-time alerts in Wazuh based on anomaly detection (triggering based on deviation from the normal baseline).
        - Set up severity levels for alerts (low, medium, high) and configure notification channels (email, dashboard alerts).
        - Visualize anomalies in Kibana with detailed dashboards and graphs.
        - Ensure easy exploration of anomalies with data filtering, drilling down into specific events.

Phase 5: Additional Use Case Testing (3 Dec – 31 Dec)

7. **17 Dec:**
    - **Advanced Use Case Testing:**
        - Test and validate additional use cases, such as:
            - Symbolic Link to Shadow Copy Created.
            - Anomalous Scheduled Tasks.
            - Unusual Remote Service Execution.
            - Abnormal Registry Changes.
        - Focus on file system, registry, and network-based anomalies.
8. **31 Dec:**
    - **Network Anomalies:**
        - Detect and monitor network-related anomalies like:
            - Unusual DNS Responses.
            - Cobalt Strike Command and Control Beacon detection.
            - NAT Traversal Port activity.
            - DNS tunneling.
        - Finalize testing and integration for network anomalies in real-time detection.

Phase 6: Performance Optimization & Final Testing (14 Jan – 28 Jan)

9. **14 Jan:**
    - **Performance Optimization:**
        - Optimize the ML models for real-time data processing without impacting system performance.
        - Ensure that real-time alerts are triggered efficiently and quickly.
        - Optimize Elasticsearch and Logstash pipelines for high performance with large data volumes.
10. **28 Jan:**
    - **System Integration Testing:**
        - Test the integration between Wazuh, ELK, and ML models in a production-like environment.
        - Simulate real-world scenarios with high volumes of log data.
        - Test the alerting mechanism across all use cases, ensuring that anomalies are detected and visualized correctly.

Phase 7: Final System Deployment & Security Audit (28 Jan – 11 Mar)

11. **11 Feb:**
    - **System Validation:**
        - Conduct a security audit on the system.
        - Verify the detection of all anomaly use cases, including logins, file creation, SMB connections, DNS activity, etc.
        - Fix any issues related to false positives or missed detections.
12. **25 Feb:**
    - **Full System Testing:**
        - Finalize the system testing, ensuring it is ready for production deployment.
        - Perform comprehensive end-to-end testing on real-time anomaly detection, visualization, and alerting.

Phase 8: Final Documentation & User Testing (11 Mar – 22 Apr)

13. **11 Mar:**
    - **Documentation:**
        - Prepare detailed documentation of the system setup, architecture, and machine learning models.
        - Include troubleshooting steps and detailed configuration guides for the Wazuh/ELK setup.
14. **25 Mar:**
    - **User Acceptance Testing (UAT):**
        - Conduct UAT with end-users to ensure the system meets functional and security requirements.
        - Refine the system based on user feedback**.**
15. **8 Apr:**
    - **User Training & Hand-off:**
        - Provide training to stakeholders on using the Kibana dashboards, interpreting alerts, and responding to security incidents.
16. **22 Apr:**
    - **Final Deployment:**
        - Deploy the system to production.
        - Ensure all components are functioning, from data collection to anomaly detection and visualization.

PHASE 9: FINAL REVIEW & PROJECT SUBMISSION (6 MAY – 20 MAY)

17. **6 May:**
    - **Project Review:**
        - Conduct a final review of the entire system.
        - Ensure that all deliverables, use cases, and security requirements are fulfilled.
        - Prepare for final submission and presentation.
18. **20 May:**
    - **Final Submission:**
        - Submit the complete project, including system demonstration, documentation, and final reports.
        - Ensure all materials (source code, datasets, models, and configurations) are well-documented and accessible.

All Topics:

- **Phase 1 (Setup & Configurations):** Install Wazuh and ELK stack, configure environments, and define use cases.
- **Phase 2-4 (Data Collection & ML Integration):** Collect real-time logs, develop and integrate AI/ML models for anomaly detection.
- **Phase 5 (Advanced Use Cases**): Test network anomalies and additional use cases.
- **Phase 6-7 (System Optimization & Testing):** Optimize, test, and finalize the anomaly detection system for production.
- **Phase 8-9 (Documentation & Submission):** Finalize documentation, conduct UAT, deploy, and submit the project.