AI-Based Cybersecurity Pipelines Project - Client Meeting Questions

2320090050

Jayakanth

# Meeting 1: Project Understanding and Scope

* What is the primary purpose of the cybersecurity pipeline (e.g., threat detection, automated response)?
* What types of data will the pipeline analyze (e.g., logs, network traffic, user behavior)?
* Should the pipeline operate in real-time, or is batch processing acceptable?
* In what environments will the pipeline be deployed (e.g., on-premises, cloud, edge)?
* Are there any regulatory or privacy constraints (e.g., GDPR) related to data handling?

# Meeting 2: Technical Specifications and Features

* Do you prefer specific models or techniques (e.g., anomaly detection, supervised learning, autoencoders)?
* Should the system handle multiple stages (e.g., data collection, detection, alerting)?
* How accurate should the threat detection be, and what level of false positives/negatives is acceptable?
* What integration points with existing systems (e.g., SIEM, firewalls) do you need?
* Is scalability important for growing cybersecurity needs?

# Meeting 3: Data Collection and Training

* What types of data (e.g., logs, network data) will be provided for model training?
* Should data augmentation techniques be applied (e.g., noise injection, balancing)?
* Do you need continuous model retraining to adapt to evolving threats?
* How will labeling of security events or anomalies be handled?
* Are there any security measures to safeguard training data (e.g., encryption)?

# Meeting 4: System Deployment and Integration

* Where will the pipeline be deployed (e.g., cloud, on-premises, hybrid)?
* Do you require a scalable system to accommodate increasing data flow and threat volume?
* Should the pipeline integrate with existing security frameworks or APIs?
* What are the expected performance benchmarks for threat detection and system response?
* Do you prefer a containerized deployment for better management and scalability (e.g., Docker, Kubernetes)?

# Meeting 5: User Experience and Feedback

* How should the system handle detected threats (e.g., alert, automated response)?
* What kind of user interface and notifications should the system provide for security teams?
* Should the system offer customizable dashboards and reports for different roles?
* What is the preferred way for users to interact with the system (e.g., web dashboard, API)?
* Will the system need to log and manage manual overrides or false positives?