Project Timeline

Packet sniffing and anomaly detection system

Project Planning & Requirements Gathering

The project planning phase focuses on establishing clear goals to build a secure API traffic monitoring system. Key tools are selected, including NGINX/Envoy for the API Gateway, Wireshark/TCPDump for packet capture, and TensorFlow/Scikit-Learn for anomaly detection.

1

API Gateway Deployment

Using NGINX or Envoy as the API Gateway, the system manages SSL decryption, rate limiting, and load balancing. Docker and Kubernetes orchestrate the microservices, with initial testing ensuring that the gateway routes traffic correctly between services.

2

Packet Sniffing Integration

Wireshark and TCPDump are installed on the gateway, capturing essential data such as IP addresses and packet sizes. This data will form the foundation for future traffic analysis and security monitoring.

3

Traffic Monitoring Setup

Basic logging is enabled in NGINX to record key metrics like IP addresses, packet sizes, and payloads. These logs provide a continuous data stream, laying the groundwork for subsequent anomaly detection.

4

Anomaly Detection System

an anomaly detection system is developed using TensorFlow or Scikit-Learn to identify unusual traffic patterns and security threats. The system detects issues like malformed requests and unauthorized access. Initial testing involves simulated anomalies to refine the detection accuracy.

5

SSL/TLS Decryption

SSL termination is configured on the gateway to decrypt API payloads for deeper analysis while ensuring privacy compliance with sensitive data.

6

API Abuse Detection & Rate Limiting

This is to manage excessive usage and prevent abuse. Using NGINX or Envoy's rate-limiting capabilities, thresholds are set to flag suspicious activity. Abuse is simulated to ensure detection rules work as intended.

7

Automated Alerting System

Automated alerting is established to notify the team in real-time of detected anomalies. Prometheus/Grafana is integrated for alert management, with rules set for various incidents. Notifications are configured via PagerDuty or other channels to ensure immediate response.

8

Traffic Logging & Auditing

Traffic data, including request/response details and timestamps, is securely logged. Splunk or Elastic Stack manages centralized log storage, and logs are integrated with a SIEM tool for effective monitoring and compliance.

9

Testing, Optimization, and Deployment

Security audits and penetration tests are conducted to identify vulnerabilities, while performance is optimized for efficiency. The project concludes with full documentation and deployment to a live environment, enabling continuous monitoring for security and performance.

10