AI-Powered Security for Cloud Containers

This presentation outlines an AI-powered security solution. It addresses the risks of running applications in Docker containers. The system detects security flaws automatically by scanning continuously and feeding the log data and the system resources to the ML model. It alerts users about potential threats, reducing risks for DevOps teams.

Problem: Container Security Risks

Software Code

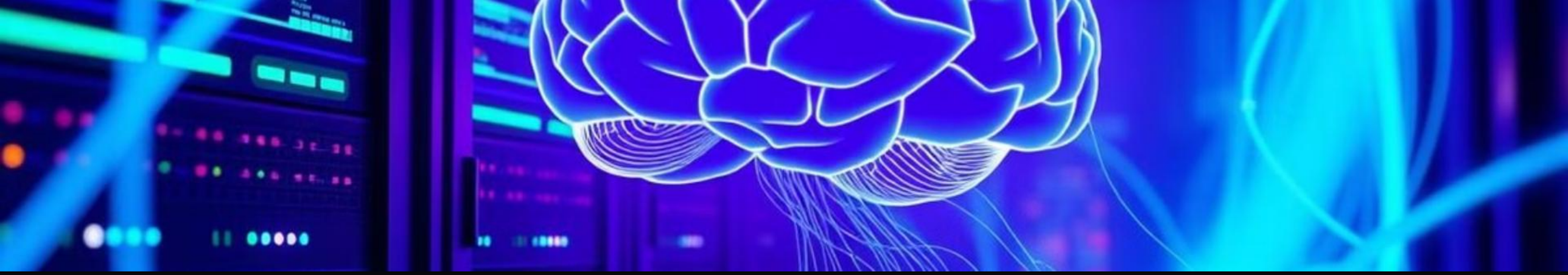
Security flaws in containerized applications can lead to breaches.

Dependencies

Vulnerabilities in libraries and dependencies are a common attack vector.

Resource Analysis

Unusual CPU, memory, or log activity indicates compromise.



Monitoring Workflow

Add Container

Enter the container's API key to begin monitoring.

Real-Time Monitoring

Continuously check logs, CPU, memory, and software vulnerabilities.

AI Anomaly Detection

Use LSTM and BERT to identify real attacks, minimizing false positives.

Security Scanning with Anchore

Vulnerability Scan

Anchore scans containers for known CVE vulnerabilities.

Critical Issue Alert

Generate alerts upon detecting critical vulnerabilities.

Alerts and Prevention

Alert

The system sends an alert to the user's dashboard.

Prevention

Suggests actions like updating OpenSSL.

Key Technologies Used

FastAPI

Handles backend API requests efficiently.

MongoDB (Atlas)

Stores user data and security alerts securely.

React

Displays real-time security alerts on the frontend.

Final Outcome: Secure Dashboard

Add Containers

Users can easily add containers for monitoring.

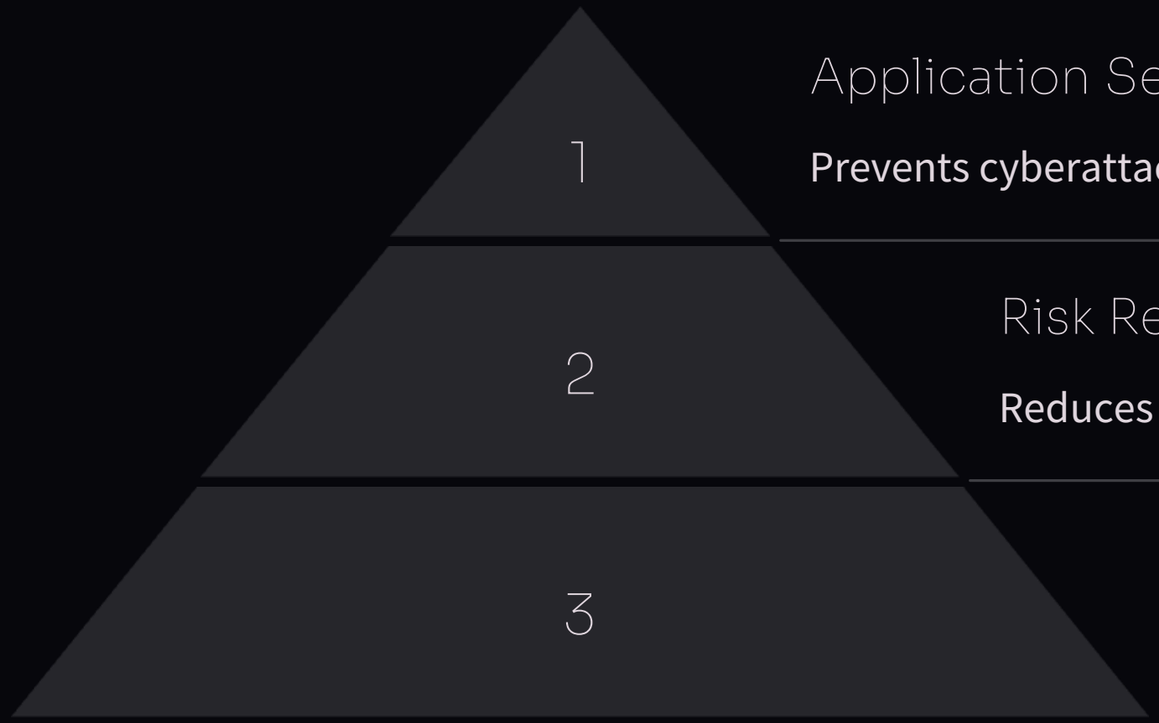
Real-time Alerts

Immediate notifications for vulnerabilities and attacks.

AI Detection

AI-based anomaly detection prevents hacking attempts.

Why This Matters



Application Security

Prevents cyberattacks on cloud applications.

Risk Reduction

Reduces security risks for DevOps teams.

Secure Deployments

Helps businesses secure software deployments.