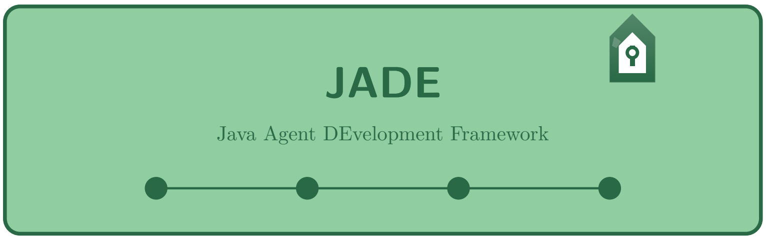
CyberSecJadeWide

Multi-Agent Cybersecurity Monitoring System



Abstract

CyberSecJadeWide is a distributed multi-agent cybersecurity monitoring system built on the JADE framework. It addresses the limitations of traditional monolithic security solutions by providing a flexible, adaptive approach to threat detection and response. The system utilizes specialized agents for monitoring, analysis, and automated response, containerized with Docker for easy deployment. This paper details the design, implementation, and results of the system, demonstrating its effectiveness in enhancing organizational security posture through real-time monitoring, anomaly detection, and automated incident response.

Background / Context

Cybersecurity monitoring systems are essential for organizations to detect and respond to security threats in real-time. Traditional monolithic approaches often lack adaptability and cannot efficiently distribute monitoring tasks across complex infrastructures. This creates an opportunity for more flexible, distributed solutions that can effectively monitor, analyze, and respond to security incidents.

Problem Statement

Current cybersecurity monitoring solutions often suffer from several limitations: they typically have centralized architectures creating single points of failure, struggle to adapt to changing threat landscapes, lack automated response capabilities, and present challenges in deployment across diverse environments. Furthermore, many solutions are not easily extensible or customizable for specific organizational needs.

Objective

CyberSecJadeWide aims to create a robust, distributed multi-agent cybersecurity monitoring system capable of detecting anomalies in system and network behavior, and automatically responding to potential security threats. The project is designed to be highly modular, containerized, and easily deployable across different environments, with real-time alerting capabilities and integration with security information and event management (SIEM) systems.

Methodology

The system is built on the JADE (Java Agent DEvelopment) framework, implementing a multi-agent architecture with three primary components:

1. **MonitorAgent**: Collects real-time system metrics (CPU, memory, disk) and network traffic data, providing a comprehensive view of system health and activities.
2. **AnalyzerAgent**: Processes metrics using statistical analysis and threshold-based detection algorithms to identify anomalies that may indicate security threats. It maintains a sliding window of metrics for continuous behavioral analysis.
3. **ResponseAgent**: Takes automated actions when anomalies are detected, including sending email alerts to security personnel, logging events to SIEM systems (Elasticsearch), and implementing firewall rules to block suspicious IP addresses.

The system is containerized using Docker, with a complete environment including Elasticsearch and Kibana for SIEM capabilities, enabling easy deployment and portability across different environments.

Results

The implemented system successfully monitors system resources and network activity, accurately detecting anomalies such as high CPU usage, memory consumption, disk utilization, and unusual network patterns. It demonstrates effective automated response through email alerting and SIEM integration, with logs and alerts available through the Kibana dashboard for security analysis. The containerized architecture ensures consistent deployment across different environments with minimal configuration.

Conclusion / Impact

CyberSecJadeWide represents a significant advancement in cybersecurity monitoring by providing a flexible, distributed approach that overcomes limitations of traditional solutions. The multi-agent architecture allows for greater resilience, adaptability, and scalability. The system's ability to detect and respond to threats in real-time reduces organizational risk and security team workload. Being open-source and extensible, it can be customized to address specific organizational security requirements and integrated with existing security infrastructure. This project demonstrates how multi-agent systems can effectively enhance cybersecurity posture with minimal overhead and maximum flexibility.

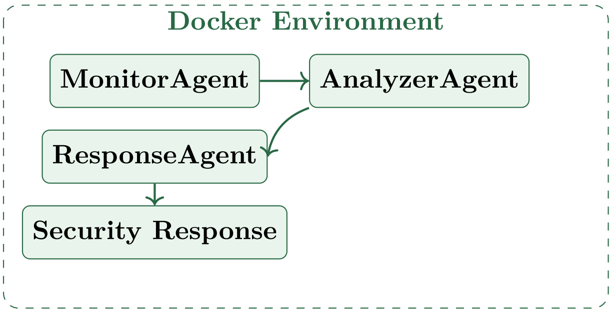


Figure 1: CyberSecJadeWide System Architecture