CLOUD-NATIVE SECURITY ARCHITECTURE PATENT

United States Patent No. US11432198

DeepShield Systems, Inc.

ABSTRACT

A system and method for providing cloud-native security architecture for industrial control systems (ICS) and operational technology (OT) environments, comprising distributed security nodes, AI-driven threat detection engines, and adaptive defense mechanisms for protecting critical infrastructure systems.

TECHNICAL FIELD

[0001] The present invention relates generally to cybersecurity systems and methods for industrial control networks, and more particularly to a cloud-native architecture for securing operational technology (OT) environments through distributed monitoring, analysis, and automated response capabilities.

BACKGROUND

[0002] Industrial control systems face increasing cybersecurity threats as operational technology networks become more connected. Traditional IT security approaches are often inadequate for OT environments due to their unique protocols, legacy systems, and operational constraints.

[0003] There remains a need for comprehensive security solutions specifically designed for industrial environments that can provide real-time threat detection and response while maintaining operational continuity.

SUMMARY OF THE INVENTION

[0004] The present invention provides a cloud-native security architecture comprising:

a) A distributed network of security monitoring nodes deployed across OT infrastructure

b) AI-driven anomaly detection engines utilizing deep learning models

c) Protocol-aware traffic analysis for industrial control systems

d) Automated incident response mechanisms with configurable policies

e) Secure communication channels between monitoring nodes and central analysis platform

DETAILED DESCRIPTION

System Architecture

[0005] The system includes the following core components:

Distributed Security Nodes

- Hardened monitoring appliances
- Local packet capture and analysis
- Protocol normalization for industrial protocols
- Secure communication channels

Central Analysis Platform

- Cloud-native deployment architecture
- Scalable data processing pipeline
- Machine learning model training and deployment
- Threat intelligence integration

Response Orchestration Engine

- Policy-based automated responses
- Configurable playbooks
- Integration with industrial control systems
- Audit logging and compliance reporting

Security Methods

[0006] The invention implements the following security methods:

Deep Packet Inspection

- Industrial protocol parsing
- Behavioral baseline establishment
- Anomaly detection
- Command validation

Machine Learning Analysis

- Supervised classification models
- Unsupervised anomaly detection
- Sequential pattern analysis
- Adaptive threshold adjustment

Response Automation

- Threat classification
- Risk scoring
- Response selection
- Action execution

CLAIMS

A cloud-native security system for industrial control networks comprising:

a) Distributed monitoring nodes

b) AI-driven analysis engines

c) Automated response mechanisms

d) Secure communication channels

The system of claim 1, wherein the monitoring nodes perform:

a) Local packet capture

b) Protocol analysis

c) Anomaly detection

d) Secure data transmission

The system of claim 1, wherein the AI engines implement:

a) Supervised learning models

b) Unsupervised detection

c) Sequential analysis

d) Adaptive thresholds

INVENTORS

- Dr. Elena Rodriguez, Chief Security Architect

- James Morrison, VP of Engineering
- Dr. Marcus Chen, Chief Executive Officer

DeepShield Systems, Inc.

PATENT DETAILS

Filing Date: March 15, 2021

Issue Date: September 20, 2022

Patent Number: US11432198

Assignee: DeepShield Systems, Inc.

Priority Date: March 15, 2020

LEGAL NOTICES

This patent document contains proprietary and confidential information of DeepShield Systems, Inc. Unauthorized reproduction or distribution of this patent document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

The technical descriptions and claims contained herein are protected under U.S. and international patent laws.

CERTIFICATION

I hereby certify that I am authorized to execute this patent document on behalf of DeepShield Systems, Inc.

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: September 20, 2022