AI-POWERED ANOMALY DETECTION ALGORITHM

United States Patent No. US11567234

ABSTRACT

A system and method for detecting anomalies in industrial control systems using artificial intelligence, comprising a multi-layered neural network architecture for real-time analysis of operational technology (OT) network traffic and system behavior patterns. The invention provides advanced threat detection capabilities through continuous learning and adaptation to evolving security threats in industrial environments.

TECHNICAL FIELD

[0001] The present invention relates generally to cybersecurity systems for industrial control networks, and more particularly to artificial intelligence-based methods for detecting anomalous behavior patterns in operational technology (OT) environments, including SCADA systems, programmable logic controllers (PLCs), and industrial automation networks.

BACKGROUND

[0002] Industrial control systems face increasingly sophisticated cyber threats that can evade traditional signature-based detection methods. Existing solutions lack the capability to effectively identify novel attack patterns and zero-day exploits in real-time while maintaining acceptable false positive rates.

[0003] There remains a need for advanced anomaly detection systems that can adapt to evolving threats while accounting for the unique characteristics and operational constraints of industrial environments.

SUMMARY OF THE INVENTION

[0004] The present invention provides an artificial intelligence-based system for detecting anomalies in industrial control networks through:

a) A multi-layered neural network architecture optimized for processing OT network traffic patterns;

b) Real-time behavioral analysis of system components using deep learning algorithms;

c) Adaptive threshold adjustment based on historical baseline data;

d) Automated classification of threat severity and attack vectors;

e) Integration with existing SCADA and PLC systems.

DETAILED DESCRIPTION

[0005] The system comprises:

Neural Network Architecture

[0006] A hierarchical neural network structure including:

- Input layer processing raw network traffic data
- Multiple hidden layers for feature extraction
- Specialized convolutional layers for pattern recognition
- Output layer for anomaly classification

Learning Algorithm

[0007] The system employs supervised and unsupervised learning mechanisms to:

- Establish baseline behavior patterns
- Identify deviations from normal operations
- Adapt to evolving threat landscapes
- Minimize false positive alerts

Integration Interface

[0008] Standard protocols for connecting with:

- SCADA systems
- PLCs and RTUs
- Industrial automation networks
- Enterprise security systems

CLAIMS

A method for detecting anomalies in industrial control systems comprising:

a) Collecting real-time network traffic data

b) Processing data through multi-layered neural networks

c) Comparing patterns against established baselines

d) Generating alerts for identified anomalies

The method of claim 1, wherein the neural network architecture includes:

a) Minimum of three hidden layers

b) Specialized convolutional filters

c) Adaptive threshold mechanisms

A system for implementing the method of claim 1, comprising:

a) Network traffic collectors

b) Processing units with GPU acceleration

c) Alert management interface

d) Integration APIs

INVENTORS

- Dr. Elena Rodriguez
- James Morrison
- Dr. Marcus Chen

ASSIGNEE

DeepShield Systems, Inc.

1234 Innovation Drive

Wilmington, DE 19801

PATENT DETAILS

Filing Date: March 15, 2021

Issue Date: January 10, 2023

Priority Date: March 15, 2020

Term: 20 years from filing date

LEGAL REPRESENTATION

Wilson & Patterson LLP

Patent Registration No. 65432

MAINTENANCE FEES

First maintenance fee due: March 15, 2024

Amount: $2,000

FOREIGN FILING RIGHTS

PCT Application No.: PCT/US2021/022456

Foreign filing deadline: March 15, 2022

CONFIDENTIALITY NOTICE

[END OF PATENT DOCUMENT]