THREAT INTELLIGENCE PROCESSING ALGORITHM PATENT

Patent No. US 11,487,623 B2

Filing Date: April 15, 2019

Issue Date: March 8, 2022

ABSTRACT

A system and method for processing industrial control system (ICS) threat intelligence data using machine learning algorithms to detect and respond to cybersecurity threats in operational technology (OT) environments. The invention comprises a novel approach to analyzing network traffic patterns, system behaviors, and threat indicators specific to industrial automation systems and SCADA networks through a multi-layered neural network architecture.

BACKGROUND OF INVENTION

Field of Invention

This invention relates to cybersecurity systems and methods, specifically to the processing and analysis of threat intelligence data in industrial control system environments using artificial intelligence and machine learning techniques.

Prior Art

Conventional threat detection systems rely primarily on signature-based detection methods and predefined rule sets, which prove insufficient for the complex and evolving nature of threats targeting industrial control systems. Existing solutions fail to adequately address the unique characteristics of OT networks and the specialized protocols used in industrial automation environments.

DETAILED DESCRIPTION

1. System Architecture

1 The system comprises:

- A primary data collection module interfacing with OT network sensors
- A preprocessing engine for normalizing and structuring raw threat data
- A deep neural network processing core with specialized industrial protocol analysis capabilities

- An automated response generation system
- A secure storage system for threat intelligence data

2 The neural network architecture implements:

- Multiple hidden layers optimized for industrial protocol analysis
- Specialized nodes for SCADA system behavior pattern recognition
- Advanced correlation engines for cross-protocol threat detection

2. Processing Methods

1 The threat intelligence processing algorithm performs the following steps:

a) Initial data ingestion from multiple OT network monitoring points

b) Protocol-specific parsing and normalization

c) Feature extraction and enhancement

d) Multi-layer pattern analysis using proprietary neural network architecture

e) Threat correlation and classification

f) Response strategy generation

2 The algorithm employs proprietary mathematical models for:

- Anomaly detection in industrial control system operations
- Behavioral analysis of OT network communications
- Prediction of potential attack vectors based on historical patterns

3. Novel Features

1 The invention includes unique capabilities for:

- Real-time analysis of industrial protocol variations
- Adaptive learning from new threat patterns
- Automated response generation specific to OT environments
- Integration with existing industrial control system architectures

4. Implementation Methods

1 The system implementation includes:

- Deployment across distributed industrial networks

- Integration with existing SCADA systems
- Secure communication channels for threat data transmission
- Scalable processing capabilities for large-scale industrial operations

CLAIMS

A method for processing threat intelligence data in industrial control system environments, comprising:

a) Collecting network traffic data from industrial control system components

b) Analyzing said data using a multi-layer neural network architecture

c) Generating automated response strategies based on threat analysis results

The method of Claim 1, wherein the neural network architecture comprises specialized nodes for industrial protocol analysis.

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

a) Data collection modules

b) Processing engines

c) Response generation systems

d) Secure storage components

INVENTORS

- Dr. Elena Rodriguez, Chief Security Architect
- James Morrison, VP of Engineering
- Sarah Blackwood, CTO

ASSIGNEE

DeepShield Systems, Inc.

1234 Innovation Drive

Wilmington, DE 19801

LEGAL REPRESENTATION

Patent prosecution handled by:

Thompson & Mitchell LLP

100 Technology Square

Boston, MA 02142

MAINTENANCE STATUS

First maintenance fee paid: September 8, 2023

Next maintenance fee due: March 8, 2026
