EUROPEAN PATENT SPECIFICATION

EP3856741 B1

MULTI-LAYER NEURAL NETWORK THREAT DETECTION SYSTEM

Publication Date: 15 March 2023

Application Number: EP21156789.3

Filing Date: 12 January 2021

Priority Date: 15 January 2020

Patent Holder: DeepShield Systems, Inc.

TECHNICAL FIELD

[0001] The present invention relates to systems and methods for detecting cyber threats in industrial control systems (ICS) and operational technology (OT) environments using a multi-layer neural network architecture. More specifically, the invention provides an adaptive threat detection framework that combines deep learning algorithms with domain-specific knowledge of industrial protocols and processes.

BACKGROUND

[0002] Industrial control systems face increasingly sophisticated cyber threats that can bypass traditional security measures. Conventional signature-based detection methods prove inadequate for identifying novel attack patterns and zero-day exploits targeting critical infrastructure.

[0003] Prior art solutions fail to effectively combine real-time analysis of network traffic with contextual understanding of industrial processes, leading to high false positive rates and delayed threat detection.

SUMMARY OF INVENTION

[0004] The present invention provides a multi-layer neural network architecture for detecting and classifying cyber threats in industrial control system environments, comprising:

(a) A primary neural network layer configured to analyze raw network traffic data using deep packet inspection;

(b) A secondary contextual layer incorporating domain knowledge of industrial protocols and expected process behaviors;

(c) A correlation engine that combines outputs from multiple analysis layers to identify threat patterns;

(d) An adaptive learning module that continuously updates threat detection models based on new attack vectors.

DETAILED DESCRIPTION

[0005] The primary neural network layer comprises:

- Input nodes processing network packets at line speed
- Multiple hidden layers for feature extraction
- Output classification nodes for initial threat scoring
- Real-time packet analysis capabilities
- Protocol-specific processing modules

[0006] The secondary contextual layer implements:

- Industrial protocol parsers for common ICS protocols
- Process behavior modeling
- State transition analysis
- Anomaly detection based on expected operations
- Cross-protocol correlation

[0007] The correlation engine performs:

- Multi-source data fusion
- Temporal pattern analysis
- Threat classification refinement
- False positive reduction
- Alert prioritization

CLAIMS

A method for detecting cyber threats in industrial control systems comprising:

(a) Receiving network traffic data from industrial control system components;

(b) Processing said data through a primary neural network layer configured to perform deep packet inspection;

(c) Analyzing industrial protocol behaviors through a secondary contextual layer;

(d) Correlating outputs from multiple analysis layers to identify threat patterns;

(e) Generating prioritized security alerts based on threat classification results.

The method of claim 1, wherein the primary neural network layer comprises at least three hidden layers implementing convolutional neural network architecture.

The method of claim 1, wherein the secondary contextual layer incorporates domain knowledge of at least five industrial protocols including Modbus, DNP3, EtherNet/IP, Profinet, and BACnet.

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

(a) Network traffic capture devices;

(b) Neural network processing units;

(c) Industrial protocol analysis modules;

(d) A correlation engine;

(e) Alert generation subsystem.

ABSTRACT

A multi-layer neural network system for detecting cyber threats in industrial control system environments is disclosed. The system combines deep packet inspection with contextual analysis of industrial protocols and processes. A primary neural network layer analyzes raw network traffic while a secondary layer incorporates domain knowledge of industrial operations. A correlation engine combines outputs to identify threat patterns while reducing false positives. The system provides adaptive threat detection capabilities specifically designed for operational technology environments.

INVENTOR

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

101 Innovation Drive

Wilmington, DE 19801

United States

PATENT REPRESENTATIVES

Johnson & Williams LLP

Patent Attorneys

1000 Technology Square

Boston, MA 02142

United States
