EUROPEAN PATENT SPECIFICATION

EP3856247 B1

Title: Multi-Layer Neural Network Threat Detection System for Industrial Control Systems

Patent Holder: DeepShield Systems, Inc.

Filing Date: March 15, 2021

Priority Date: March 15, 2020

Grant Date: September 30, 2023

TECHNICAL FIELD

[0001] The present invention relates to cybersecurity systems for industrial control networks, and more particularly to a multi-layer neural network architecture for detecting and classifying cyber threats in operational technology (OT) environments.

BACKGROUND

[0002] Industrial control systems (ICS) and operational technology networks face increasingly sophisticated cyber threats that can evade traditional signature-based detection methods. Existing solutions lack the capability to effectively identify zero-day attacks and novel threat patterns in real-time without disrupting critical industrial processes.

[0003] Prior art solutions typically rely on single-layer analysis or rule-based detection, which cannot adequately address the complexity of modern industrial cyber threats.

SUMMARY OF INVENTION

[0004] The invention provides a multi-layer neural network system for detecting cyber threats in industrial control networks comprising:

a) A first neural network layer configured to analyze raw network traffic data from industrial control system protocols including Modbus, DNP3, and proprietary SCADA protocols;

b) A second neural network layer implementing pattern recognition algorithms to identify anomalous behavior patterns across multiple industrial control system nodes;

c) A third neural network layer utilizing deep learning techniques to classify detected anomalies and determine threat severity;

d) An automated response module capable of implementing defensive measures without disrupting critical industrial processes.

DETAILED DESCRIPTION

[0005] The first neural network layer comprises:

- Protocol-specific traffic analyzers
- Packet inspection modules
- Traffic flow correlation engines
- Baseline behavior modeling components

[0006] The second neural network layer implements:

- Multi-node behavior pattern analysis
- Temporal correlation of events
- Process variable tracking
- Control loop monitoring

[0007] The third neural network layer provides:

- Threat classification using supervised learning
- Severity assessment algorithms
- False positive reduction
- Attack chain analysis

CLAIMS

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

a) Collecting network traffic data from industrial control system protocols;

b) Processing said data through multiple neural network layers;

c) Classifying anomalies using machine learning algorithms;

d) Implementing automated defensive responses.

The method of claim 1 wherein the neural network layers comprise:

a) A protocol analysis layer;

b) A pattern recognition layer;

c) A threat classification layer.

The method of claim 1 further comprising:

a) Real-time monitoring of industrial process variables;

b) Correlation of events across multiple control system nodes;

c) Automated response actions that maintain process stability.

TECHNICAL ADVANTAGES

[0008] The invention provides several advantages over prior art:

- Improved detection of zero-day threats
- Reduced false positive rates
- Minimal impact on industrial processes
- Automated threat response capabilities
- Scalability across large industrial networks

INDUSTRIAL APPLICABILITY

[0009] The invention is particularly applicable to:

- Critical infrastructure protection
- Manufacturing facilities
- Energy production systems
- Maritime installations
- Chemical processing plants

PATENT FAMILY INFORMATION

Related Applications:

- US Patent Application No. 17/204,568
- PCT Application No. PCT/US2021/022445

Priority Claims:

- US Provisional Application No. 63/124,890

LEGAL NOTICES

CERTIFICATION

I hereby certify that this is a true and accurate copy of European Patent EP3856247 B1 as granted by the European Patent Office.

/s/ Elena Rodriguez

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: September 30, 2023

AUTHENTICATION

European Patent Office Reference Number: EPO-2023-85624701

Authentication Code: 7F9A2B4D5E8C3F6