PATENT CERTIFICATE

Patent No. CN112567890

Real-time Threat Analysis Algorithm for Industrial Control Systems

PATENT HOLDER: DeepShield Systems, Inc.

FILING DATE: March 15, 2019

ISSUE DATE: September 22, 2020

JURISDICTION: People's Republic of China

CLASSIFICATION: G06F 21/55, G06N 20/00

ABSTRACT

A system and method for real-time threat analysis in industrial control systems utilizing machine learning algorithms to detect and respond to cybersecurity threats in operational technology (OT) environments. The invention comprises a multi-layered neural network architecture that processes network traffic data, system logs, and sensor readings to identify anomalous patterns indicative of cyber threats or system compromises.

TECHNICAL FIELD

This invention relates to the field of industrial cybersecurity, specifically concerning:

Real-time monitoring of industrial control system (ICS) networks

Artificial intelligence-based threat detection

Automated response mechanisms for OT security incidents

SCADA system protection

Maritime and subsea infrastructure security systems

CLAIMS

A method for real-time threat analysis in industrial control systems, comprising:

a) Collecting real-time data streams from multiple ICS sensors and control points;

b) Processing collected data through a proprietary three-tier neural network architecture;

c) Implementing pattern recognition algorithms specifically calibrated for OT environments;

d) Generating threat signatures based on detected anomalies;

e) Executing automated response protocols based on threat classification.

The system architecture as claimed in Claim 1, further comprising:

a) A primary analysis layer utilizing supervised learning algorithms;

b) A secondary verification layer employing unsupervised anomaly detection;

c) A tertiary response layer incorporating reinforcement learning capabilities.

The method of Claim 1, wherein the threat analysis algorithm includes:

a) Real-time processing capabilities with latency under 50 milliseconds;

b) Adaptive learning mechanisms for evolving threat patterns;

c) Integration with standard ICS protocols including Modbus, DNP3, and IEC 61850.

DETAILED DESCRIPTION

1. System Architecture

The patented system comprises a distributed architecture with the following components:

1 Data Collection Module

- Network traffic monitors
- System log aggregators
- Industrial sensor interfaces
- Control system integration points

2 Analysis Engine

- Primary neural network layer
- Secondary verification system
- Threat signature database
- Pattern matching algorithms

3 Response Module

- Automated containment protocols
- Alert generation system
- Incident response automation
- System restoration procedures

2. Technical Specifications

1 Processing Requirements

- Minimum processing capability: 100,000 events per second
- Maximum latency: 50 milliseconds
- Scalability: Up to 1,000 monitored nodes per instance

2 Implementation Parameters

- Compatible with standard ICS protocols
- Supports air-gapped environments
- Integrates with existing SIEM systems
- Provides REST API interfaces

3. Novel Features

1 The invention introduces several novel features:

- Adaptive learning algorithms specific to OT environments
- Real-time threat signature generation
- Automated response calibration
- Maritime-specific threat detection modules

LEGAL NOTICES

1. Patent Rights

All rights, title, and interest in this patent are owned exclusively by DeepShield Systems, Inc. This patent is protected under international patent laws and treaties.

2. Restrictions

No license, either expressed or implied, is granted under any patent right or other intellectual property right of DeepShield Systems, Inc. Any unauthorized use, reproduction, or distribution is strictly prohibited.

3. Term

This patent shall remain in force for a period of 20 years from the filing date, subject to payment of maintenance fees and absence of invalidation.

CERTIFICATION

This patent certificate accurately represents the claims and specifications as approved by the China National Intellectual Property Administration.

Patent Examiner: [ ]

Registration Number: [PE2020-7789]

Official Seal Applied: [SEAL]

Executed this 22nd day of September, 2020

/s/ Marcus Chen

_

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

/s/ Elena Rodriguez

_

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.