UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US11245632

Real-Time Threat Classification System for Industrial Control Networks

Issue Date: March 15, 2023

Application No.: 16/789,432

Filing Date: February 12, 2021

Assignee: DeepShield Systems, Inc., Wilmington, Delaware

Inventors: Chen, Marcus; Rodriguez, Elena; Morrison, James

ABSTRACT

A system and method for real-time classification of cyber threats in industrial control system (ICS) networks utilizing machine learning algorithms and behavioral analysis. The invention comprises a multi-layered detection architecture that processes network traffic patterns, operational technology (OT) protocol behaviors, and system state variations to identify and categorize potential security threats with minimal latency. The system employs proprietary neural network models specifically trained on industrial control system protocols and operational patterns.

CLAIMS

A method for real-time threat classification in industrial control networks, comprising:

a) receiving network traffic data from multiple ICS network segments;

b) analyzing said network traffic using at least one machine learning model trained on industrial protocol patterns;

c) generating behavioral fingerprints for normal operational states;

d) detecting deviations from established behavioral baselines;

e) classifying detected anomalies using a hierarchical threat classification framework;

f) implementing automated response protocols based on threat classification results.

The method of claim 1, wherein the machine learning model comprises:

a) a deep neural network architecture optimized for OT protocol analysis;

b) multiple classification layers for protocol-specific behavior analysis;

c) real-time feature extraction capabilities;

d) adaptive learning mechanisms for continuous model improvement.

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

a) network sensors deployed across ICS infrastructure;

b) a central processing unit executing the machine learning models;

c) memory storage containing behavioral baseline data;

d) a threat classification engine;

e) an automated response module.

DETAILED DESCRIPTION

Background

Industrial control systems face increasingly sophisticated cyber threats requiring advanced detection and classification capabilities. Traditional signature-based detection methods prove insufficient for identifying novel attack patterns and zero-day exploits. This invention addresses these limitations through innovative application of machine learning and behavioral analysis techniques specifically designed for ICS environments.

Technical Implementation

The system implements a multi-stage processing pipeline:

Data Collection Layer

- Distributed network sensors
- Protocol-specific traffic capture
- State monitoring agents
- Operational metrics collection

Analysis Layer

- Real-time traffic processing
- Protocol behavior analysis
- State transition monitoring
- Pattern matching algorithms

Classification Layer

- Threat categorization engine
- Confidence scoring mechanism
- Impact assessment module
- Response recommendation system

Novel Features

The invention incorporates several innovative elements:

Protocol-Aware Neural Networks

- Specialized architecture for ICS protocols
- Optimized processing for real-time analysis
- Adaptive learning capabilities

Behavioral Baseline Generation

- Automated learning of normal operations
- Dynamic baseline updates
- Multi-dimensional state modeling

Threat Classification Framework

- Hierarchical threat categorization
- Context-aware risk assessment
- Automated response selection

INDUSTRIAL APPLICABILITY

This invention provides particular utility in:

- Critical infrastructure protection
- Manufacturing operations security

- Maritime facility cybersecurity
- Energy sector operations
- Industrial automation environments

PRIOR ART REFERENCES

US Patent 10,892,916

US Patent 10,747,606

US Patent Application 2020/0162503

EP Patent 3,456,789

LEGAL NOTICES

The described invention is protected under United States patent law and applicable international treaties. Any use of the described methods and systems requires explicit written permission from DeepShield Systems, Inc.

EXECUTION

Granted this 15th day of March, 2023

[SIGNATURE BLOCK]

United States Patent and Trademark Office

Alexandria, Virginia

[SEAL]