UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US11234567

Behavioral Analysis Engine for Industrial Control System Security

Issue Date: March 15, 2023

Filing Date: April 12, 2021

Priority Date: April 15, 2020

Assignee: DeepShield Systems, Inc.

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

Term: 20 years from filing date

ABSTRACT

A system and method for real-time behavioral analysis of industrial control system (ICS) networks utilizing machine learning algorithms to detect and respond to cybersecurity threats. The invention comprises a multi-layered analysis engine that monitors operational technology (OT) network traffic, establishes behavioral baselines, and identifies anomalous patterns indicative of potential security breaches or system compromises.

CLAIMS

A method for securing industrial control systems comprising:

a) collecting real-time network traffic data from industrial control system components;

b) analyzing said network traffic using a multi-layer neural network architecture configured to:

- establish baseline operational patterns
- detect deviations from normal behavior
- classify potential threats based on predetermined risk factors
- generate automated response protocols

c) implementing protective measures through:

- network segmentation
- traffic filtering

- command validation
- protocol enforcement

The method of claim 1, wherein the neural network architecture comprises:

a) A primary analysis layer utilizing supervised learning algorithms trained on:

- known attack patterns
- legitimate operational sequences
- vendor-specific protocol characteristics

b) A secondary analysis layer implementing unsupervised learning for:

- pattern recognition
- anomaly detection
- behavioral clustering

A system for implementing the method of claim 1 comprising:

a) Network sensors deployed at critical infrastructure points

b) A centralized processing engine incorporating:

- Data collection modules
- Analysis algorithms
- Response generators

c) Integration interfaces for:

- SCADA systems
- PLCs
- Industrial protocols
- Security infrastructure

DETAILED DESCRIPTION

Background

Industrial control systems face increasing cybersecurity threats requiring advanced detection and response capabilities. Traditional signature-based security measures prove insufficient for protecting complex OT environments. This invention provides a comprehensive solution through behavioral analysis and machine learning.

Technical Implementation

The behavioral analysis engine utilizes a proprietary neural network architecture specifically designed for industrial environments. The system processes network traffic data through multiple analytical layers:

Protocol Analysis Layer

- Validates communication patterns
- Enforces protocol specifications
- Identifies unauthorized commands

Behavioral Modeling Layer

- Establishes operational baselines
- Tracks system state changes
- Maps normal interaction patterns

Threat Detection Layer

- Applies machine learning algorithms
- Evaluates anomaly significance
- Generates threat classifications

System Components

The invention comprises the following core components:

Data Collection Framework

- Network traffic capture
- Protocol parsing
- State tracking
- Event logging

Analysis Engine

- Neural network processor
- Pattern matching system

- Behavioral modeling unit
- Threat classification module

Response System

- Alert generation
- Automated countermeasures
- System isolation protocols
- Recovery procedures

INDUSTRIAL APPLICABILITY

This invention provides critical protection for:

- Manufacturing facilities
- Power generation plants
- Water treatment facilities
- Oil and gas infrastructure
- Maritime operations
- Transportation systems

LEGAL NOTICES

This patent document contains proprietary information owned by DeepShield Systems, Inc. All rights reserved. Unauthorized reproduction or distribution is prohibited.

The described invention is protected under U.S. Patent Law and may be subject to additional pending patent applications. Any use of the described methods or systems requires explicit written permission from DeepShield Systems, Inc.

CERTIFICATION

I hereby certify that this patent document accurately describes the invention as implemented by DeepShield Systems, Inc.

Dated: March 15, 2023

/s/ Elena Rodriguez, Ph.D.

Chief Security Architect

DeepShield Systems, Inc.

/s/ James Morrison

VP of Engineering

DeepShield Systems, Inc.