UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US10984522 B2

DeepShield Core Architecture for Industrial Control System Security

Filed: March 15, 2018

Issued: April 20, 2021

Assignee: DeepShield Systems, Inc.

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

ABSTRACT

A system and method for securing industrial control systems through a multi-layered security architecture incorporating deep learning-based anomaly detection, real-time threat monitoring, and automated response mechanisms. The invention provides comprehensive protection for operational technology (OT) environments by implementing a novel approach to industrial network security using proprietary algorithms for pattern recognition and threat mitigation in SCADA systems and industrial automation networks.

CLAIMS

A method for securing industrial control systems comprising:

a) implementing a multi-layer security architecture comprising:

- a deep packet inspection (DPI) engine optimized for industrial protocols
- a neural network-based anomaly detection system
- a real-time threat correlation engine
- an automated response orchestration module

b) wherein said architecture:

- monitors industrial network traffic in real-time
- analyzes control system commands and responses
- identifies unauthorized access attempts and anomalous behavior
- implements protective measures without disrupting critical operations

The method of claim 1, wherein the deep packet inspection engine:

a) decodes and analyzes industrial protocols including:

- Modbus TCP/IP
- EtherNet/IP
- Profinet
- DNP3
- IEC 61850

b) maintains protocol state information

c) validates command sequences and parameters

The method of claim 1, wherein the neural network-based anomaly detection:

a) utilizes a hybrid architecture combining:

- supervised learning for known threat patterns
- unsupervised learning for novel attack detection
- reinforcement learning for response optimization

b) maintains separate behavioral baselines for:

- network traffic patterns
- control system operations
- process parameters
- user activities

DETAILED DESCRIPTION

Background

Industrial control systems face increasing cybersecurity threats as operational technology networks become more connected. Traditional IT security solutions are insufficient for protecting critical infrastructure and industrial operations. This invention addresses these challenges through a specialized security architecture designed specifically for industrial environments.

Technical Implementation

The core architecture comprises four primary components:

Industrial Protocol Analysis Engine

- Custom protocol dissectors for industrial communications
- State tracking and command validation
- Protocol-specific security policy enforcement

Deep Learning Security Module

- Multi-layer neural network architecture
- Real-time pattern analysis and anomaly detection
- Adaptive learning capabilities

Threat Intelligence Framework

- Industrial threat intelligence integration
- Attack pattern correlation
- Risk scoring and prioritization

Response Orchestration System

- Automated threat mitigation
- Configurable response actions
- Operation impact analysis

Novel Features

The invention includes several innovative elements:

Protocol-Aware Security

- Industrial protocol-specific security rules
- Command sequence validation
- Parameter boundary checking

Adaptive Learning System

- Continuous baseline updates
- Dynamic threat model adaptation
- Automated response optimization

Operational Context Integration

- Process-aware security policies
- Safety system integration

- Production impact analysis

INDUSTRIAL APPLICABILITY

This invention is particularly applicable to:

- Critical infrastructure protection
- Manufacturing operations
- Energy production facilities
- Maritime installations
- Transportation systems
- Utility operations

LEGAL NOTICES

This patent and all rights thereunder are owned exclusively by DeepShield Systems, Inc. Any unauthorized use, reproduction, or distribution of the described technology may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

CERTIFICATION

I hereby certify that I am authorized to execute this patent application on behalf of DeepShield Systems, Inc.

/s/ Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.

Date: March 15, 2018

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: March 15, 2018