UNITED STATES PATENT

Patent No. US11134567

INDUSTRIAL CONTROL SYSTEM PROTECTION METHOD AND SYSTEM

Issue Date: March 15, 2023

Application No.: 16/789,432

Filing Date: September 12, 2020

Assignee: DeepShield Systems, Inc., Delaware

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

ABSTRACT

A system and method for protecting industrial control systems through multi-layered security architecture incorporating artificial intelligence-driven threat detection and response mechanisms. The invention provides comprehensive protection for operational technology (OT) environments through real-time monitoring, behavioral analysis, and automated incident response protocols specifically designed for industrial automation systems and SCADA networks.

CLAIMS

A method for protecting industrial control systems, comprising:

a) implementing a deep-layer security architecture comprising:

- a primary monitoring layer for OT network traffic analysis
- a secondary behavioral analysis layer utilizing machine learning algorithms
- a tertiary response layer incorporating automated defense mechanisms

b) establishing baseline operational parameters through:

- continuous monitoring of normal system operations
- cataloging standard communication patterns
- mapping authorized control sequences

c) detecting anomalous behavior via:

- real-time comparison against established baselines
- pattern recognition using neural network analysis
- correlation of multiple threat indicators

The method of claim 1, wherein the deep-layer security architecture further comprises:

a) A proprietary AI engine that:

- processes network traffic data in real-time
- identifies potential threats using predictive analytics
- generates automated response protocols

b) Specialized modules for:

- maritime infrastructure protection
- subsea system security
- industrial automation defense

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

a) Network monitoring components including:

- dedicated OT traffic analyzers
- protocol-specific decoders
- encrypted communication channels

b) Processing units configured to:

- execute machine learning algorithms
- maintain threat intelligence databases
- coordinate response actions

DETAILED DESCRIPTION

The present invention relates to advanced cybersecurity systems specifically designed for industrial control system (ICS) environments. The system implements a novel approach to protecting critical infrastructure through multi-layered security architecture that combines traditional network monitoring with artificial intelligence-driven threat detection and response capabilities.

Technical Field

The invention operates within the technical field of industrial cybersecurity, specifically addressing the unique challenges of protecting operational technology (OT) environments, SCADA systems, and industrial automation networks. The system is particularly adapted for use in maritime facilities, offshore energy platforms, and manufacturing enterprises with complex OT environments.

Background

Prior art solutions have typically focused on traditional IT security approaches that fail to address the unique requirements of industrial control systems. This invention overcomes these limitations through specialized protocols and architectures specifically designed for OT environments.

Detailed Implementation

The system comprises three primary components:

Deep-Layer Monitoring System

- Continuous network traffic analysis
- Protocol-specific monitoring
- Behavioral baseline establishment

AI-Driven Analysis Engine

- Machine learning algorithms for pattern recognition
- Predictive analytics for threat detection
- Automated anomaly classification

Response Mechanism

- Automated threat mitigation
- Incident response coordination
- System recovery protocols

INDUSTRIAL APPLICABILITY

This invention provides particular utility in:

- Maritime facility protection
- Offshore platform security
- Manufacturing environment defense
- Critical infrastructure safeguarding

- Industrial automation security

LEGAL NOTICES

This patent document contains proprietary information owned by DeepShield Systems, Inc. All rights reserved. Unauthorized reproduction or distribution of this patent or any portion of it may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Patent Attorneys of Record:

Morrison & Foerster LLP

2000 Pennsylvania Avenue, NW

Washington, DC 20006-1888

For: DeepShield Systems, Inc.

Two Commerce Square

2001 Market Street, Suite 2800

Philadelphia, PA 19103