UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US10897654

Automated Incident Response System for Industrial Control Networks

Issue Date: March 15, 2022

Filing Date: April 3, 2019

Priority Date: April 5, 2018

Assignee: DeepShield Systems, Inc.

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

Term: 20 years from filing date

ABSTRACT

A system and method for automated incident response in industrial control networks comprising a multi-layered detection and response architecture that utilizes artificial intelligence to identify and mitigate cyber threats in operational technology (OT) environments. The system includes specialized modules for real-time monitoring of industrial protocols, anomaly detection using machine learning algorithms, and automated response mechanisms calibrated for critical infrastructure protection.

CLAIMS

An automated incident response system for industrial control networks comprising:

a) A network monitoring subsystem configured to:

- Capture and analyze industrial protocol traffic in real-time
- Monitor operational parameters across distributed control systems
- Maintain baseline behavioral profiles for connected devices

b) An artificial intelligence engine configured to:

- Process network telemetry using deep learning algorithms
- Detect anomalous patterns indicating potential security threats
- Classify incidents based on threat severity and impact

c) An automated response module configured to:

- Execute pre-defined response protocols based on threat classification
- Implement network segmentation and containment measures
- Generate incident reports and forensic data

The system of claim 1, wherein the network monitoring subsystem includes:

- Protocol-specific parsers for industrial control protocols
- Distributed sensors for OT network visibility
- Encrypted communication channels between components

The system of claim 1, wherein the artificial intelligence engine comprises:

- Neural network models trained on industrial threat data
- Real-time pattern matching algorithms
- Adaptive learning capabilities for threat evolution

The system of claim 1, wherein the automated response module includes:

- Configurable response policies
- Integration with industrial firewall systems
- Automated workflow triggers for incident management

DETAILED DESCRIPTION

Technical Field

The present invention relates to cybersecurity systems for industrial control networks, specifically to automated incident response mechanisms designed to protect operational technology environments from cyber threats while maintaining operational continuity.

Background

Industrial control systems face increasing cybersecurity threats that can impact critical infrastructure operations. Traditional security approaches are insufficient for OT environments due to their unique operational requirements and protocols. This invention addresses these challenges through an innovative approach to threat detection and automated response.

System Architecture

The system comprises three primary components:

Network Monitoring Layer

- Distributed sensors deployed across OT networks
- Protocol-specific traffic analysis engines
- Real-time operational data collection

AI Analysis Engine

- Deep learning models for threat detection
- Behavioral analysis algorithms
- Pattern recognition systems

Response Automation Layer

- Policy-driven response mechanisms
- Containment and mitigation workflows
- Incident documentation and reporting

Implementation Methods

The system implements a multi-stage approach to incident response:

Continuous Monitoring

- Protocol-level traffic analysis
- Operational parameter tracking
- Baseline profile maintenance

Threat Detection

- AI-driven anomaly detection
- Threat classification
- Impact assessment

Automated Response

- Graduated response protocols
- Containment measures
- Recovery procedures

INDUSTRIAL APPLICABILITY

This invention is particularly applicable to:

- Critical infrastructure protection
- Industrial automation systems
- SCADA networks
- Manufacturing operations
- Maritime control systems

LEGAL NOTICES

Patent Attorney of Record:

Sarah J. Williams, Reg. No. 58,432
Williams & Associates, LLP
100 Technology Square
Boston, MA 02142

Correspondence Address:

DeepShield Systems, Inc.
Legal Department - Patents
2500 Innovation Drive
Wilmington, DE 19801

[END OF PATENT DOCUMENT]