UNITED STATES PATENT AND TRADEMARK OFFICE

Patent No. US11567890

Threat Intelligence Feed Processing System and Method for Industrial Control Systems

Issue Date: March 15, 2023

Filing Date: April 12, 2021

Priority Date: April 15, 2020

Assignee: DeepShield Systems, Inc.

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

Attorney Docket No.: DSS-2021-PTN-0023

ABSTRACT

A system and method for processing threat intelligence feeds in industrial control system (ICS) environments, comprising a specialized feed aggregation engine, machine learning-based classification system, and automated response framework. The invention provides real-time analysis of multiple threat intelligence sources, correlation with operational technology (OT) network traffic patterns, and automated implementation of defensive measures specifically adapted for industrial automation systems and SCADA networks.

CLAIMS

A method for processing threat intelligence feeds in industrial control systems, comprising:

a) receiving threat intelligence data from multiple external feeds;

b) aggregating and normalizing said threat intelligence data through a specialized processing engine;

c) analyzing said normalized data using machine learning algorithms trained on industrial control system attack patterns;

d) correlating identified threats with real-time operational technology network traffic;

e) automatically generating and implementing defensive measures based on threat correlation results.

The method of claim 1, wherein said machine learning algorithms comprise:

a) deep neural networks trained on industrial protocol behaviors;

b) anomaly detection models specific to SCADA systems;

c) pattern recognition algorithms for identifying attack signatures in OT environments.

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

a) a feed aggregation module;

b) a machine learning classification engine;

c) a correlation analysis subsystem;

d) an automated response framework;

e) integration interfaces for industrial control system environments.

DETAILED DESCRIPTION

Background

Industrial control systems face increasingly sophisticated cyber threats requiring advanced detection and response capabilities. Traditional threat intelligence processing methods lack specific adaptations for OT environments and industrial protocols. This invention addresses these limitations through specialized feed processing and automated response mechanisms.

Technical Implementation

The system implements a multi-layer architecture comprising:

Feed Collection Layer

- Protocol-specific collectors for various intelligence sources
- Data normalization and standardization components
- Feed validation and integrity checking mechanisms

Analysis Layer

- Machine learning classification engine
- Pattern matching subsystem
- Behavioral analysis module

- Industrial protocol decoders

Response Layer

- Automated rule generation
- Defense measure implementation
- System integration interfaces

Novel Features

The invention incorporates several novel technical elements:

Specialized processing algorithms for industrial protocol analysis

Machine learning models trained specifically on OT attack patterns

Automated response mechanisms adapted for industrial environments

Integration capabilities with existing SCADA systems

INDUSTRIAL APPLICABILITY

This invention has direct application in:

Manufacturing facilities

Power generation plants

Water treatment facilities

Oil and gas operations

Maritime infrastructure

Critical infrastructure protection

TECHNICAL ADVANTAGES

The invention provides:

Reduced false positive rates through OT-specific analysis

Faster threat detection and response times

Improved integration with industrial control systems

Enhanced protection against sophisticated attacks

Reduced operational impact during threat response

LEGAL NOTICES

CERTIFICATION

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

Executed this 12th day of April, 2021

/s/ Elena Rodriguez

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

/s/ James Morrison

James Morrison

VP of Engineering

DeepShield Systems, Inc.

/s/ Marcus Chen

Dr. Marcus Chen

Chief Executive Officer

DeepShield Systems, Inc.