NETWORK TRAFFIC ANALYSIS SYSTEM PATENT

United States Patent No. US11245633

DeepShield Systems, Inc.

ABSTRACT

A system and method for analyzing network traffic in industrial control system (ICS) environments using machine learning-based pattern recognition and anomaly detection. The invention provides real-time monitoring and analysis of operational technology (OT) network communications to identify potential security threats and operational anomalies in critical infrastructure environments.

TECHNICAL FIELD

[001] The present invention relates generally to cybersecurity systems and methods for industrial control networks, and more particularly to an artificial intelligence-driven system for analyzing network traffic patterns in operational technology (OT) environments to detect potential security threats and system anomalies.

BACKGROUND

[002] Industrial control systems face increasing cybersecurity threats as operational technology networks become more connected. Traditional IT security solutions are often inadequate for protecting specialized industrial protocols and control system architectures. There exists a need for sophisticated network traffic analysis capabilities specifically designed for industrial environments.

[003] Prior approaches have failed to adequately address the unique challenges of monitoring industrial network traffic while maintaining operational continuity. This invention provides novel methods for deep packet inspection and behavioral analysis of industrial protocols without impacting critical system operations.

SUMMARY OF THE INVENTION

[004] The present invention provides systems and methods for monitoring and analyzing network traffic in industrial control system environments using machine learning and artificial intelligence techniques. Key components include:

[005] A network traffic capture system optimized for industrial protocols including Modbus, DNP3,

BACnet, and proprietary control system communications

[006] Machine learning models trained on normal operational patterns to detect anomalous behavior

[007] Real-time analysis engine for identifying potential security threats and operational issues

[008] Automated response capabilities for containing detected threats while maintaining operational continuity

DETAILED DESCRIPTION

[009] The system comprises multiple integrated components working together to provide comprehensive network traffic analysis:

Traffic Capture Module

[010] Specialized network taps and packet capture devices designed for industrial networks

[011] Protocol-aware filtering and preprocessing

[012] Lossless packet capture at line rates up to 100Gbps

[013] Support for both standard and proprietary industrial protocols

Analysis Engine

[014] Machine learning models for behavioral analysis

[015] Pattern matching against known threat signatures

[016] Statistical analysis of traffic flows and protocol behaviors

[017] Correlation engine for identifying complex attack patterns

Response Framework

[018] Automated threat containment capabilities

[019] Integration with existing security infrastructure

[020] Configurable response policies

[021] Audit logging and forensics support

CLAIMS

A method for analyzing network traffic in industrial control systems comprising:

a) Capturing network packets using protocol-aware collection devices

b) Analyzing traffic patterns using machine learning models

c) Detecting anomalous behavior and security threats

d) Initiating automated response actions

The method of claim 1 wherein the machine learning models are trained on:

a) Normal operational patterns

b) Known attack signatures

c) Protocol-specific behaviors

d) Historical traffic profiles

A system for implementing the method of claim 1 comprising:

a) Network tap devices

b) Analysis engines

c) Response modules

d) Management interface

INVENTORS

- Dr. Elena Rodriguez
- James Morrison
- Dr. Marcus Chen

ASSIGNEE

DeepShield Systems, Inc.

1234 Innovation Drive

Dover, Delaware 19901

PATENT DETAILS

Filing Date: March 15, 2021

Issue Date: February 8, 2022

Patent Number: US11245633

Priority Date: March 15, 2020

LEGAL NOTICES

This patent document contains proprietary and confidential information belonging to DeepShield Systems, Inc. Any unauthorized use, reproduction, or distribution is strictly prohibited and may result in severe civil and criminal penalties.

The technical implementations described herein may be subject to various other patents, trademarks, and/or copyrights owned by DeepShield Systems, Inc. and others. All rights are reserved.

CERTIFICATION

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

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: February 8, 2022