OT/IT Convergence Security Framework Patent EP3812456

European Patent Specification

Publication Date: 15 March 2023

Patent Number: EP3812456

Application Number: EP20198765.4

Title of Invention

System and Method for Securing Converged Operational Technology and Information Technology Networks Using Adaptive Defense Architecture

Patent Holder

DeepShield Systems, Inc.

1209 North Orange Street

Wilmington, Delaware 19801

United States of America

Technical Field

[001] The present invention relates to cybersecurity systems and methods for protecting industrial control systems (ICS) and operational technology (OT) networks, particularly in environments where OT systems interface with traditional information technology (IT) infrastructure. More specifically, the invention provides an adaptive security framework for detecting and mitigating threats in converged OT/IT environments using artificial intelligence and machine learning techniques.

Background

[002] Industrial control systems increasingly require integration with enterprise IT networks, creating new security vulnerabilities at the convergence points. Traditional IT security solutions are inadequate for protecting OT environments due to their unique operational requirements and protocols.

[003] Prior art solutions have failed to address the specific challenges of securing OT/IT interfaces while maintaining operational continuity and real-time response capabilities required in industrial environments.

Summary of Invention

[004] The invention provides a novel security framework comprising:

a) An AI-driven threat detection engine specifically calibrated for OT protocols and behaviors

b) Real-time monitoring system for converged OT/IT network traffic

c) Adaptive defense mechanisms that automatically adjust security policies based on threat context

d) Specialized protection for industrial protocols including Modbus, DNP3, and IEC-61850

e) Neural network-based anomaly detection optimized for industrial process patterns

Detailed Description

[005] The security framework implements a multi-layer architecture:

Layer 1: Protocol Analysis

[006] Proprietary deep packet inspection engine processes both IT and OT protocol traffic, maintaining separate processing paths while identifying cross-domain threats.

Layer 2: Behavioral Analytics

[007] Machine learning models baseline normal operational patterns across both OT and IT systems, detecting anomalous activities that may indicate compromise.

Layer 3: Adaptive Response

[008] Context-aware defense mechanisms automatically implement appropriate countermeasures based on threat classification and operational impact assessment.

Claims

A method for securing converged OT/IT networks comprising:

a) Monitoring network traffic using protocol-aware sensors

b) Analyzing traffic patterns using machine learning models

c) Implementing adaptive security policies based on threat context

d) Maintaining operational continuity during threat response

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

a) Historical process data from industrial operations

b) Known attack patterns and signatures

c) Normal operational baselines

d) Equipment-specific behavioral profiles

A system implementing the method of claims 1-2, comprising:

a) Network sensors deployed at OT/IT convergence points

b) Central analysis engine with AI/ML capabilities

c) Policy enforcement modules

d) Automated response mechanisms

Technical Implementation

[009] The invention is implemented using:

- Distributed network sensors with specialized OT protocol support
- Centralized analysis engine using TensorFlow-based neural networks
- Custom-developed machine learning models for industrial process analysis
- Hardened security policy enforcement points
- Encrypted command and control channels

Patent Term

[010] This patent shall remain in force for a period of 20 years from the filing date of March 15, 2020, subject to payment of prescribed maintenance fees.

Assignment Rights

[011] All rights, title and interest in this patent are owned exclusively by DeepShield Systems, Inc., including the right to sue for past, present and future infringement.

Certification

[012] This patent document accurately reflects the claims and specifications as approved by the European Patent Office.

Authentication

European Patent Office Reference Number: EPO-2020-198765

Validation Code: DS789321EP

Issue Date: March 15, 2023

Authorized Representative:

Elena Rodriguez, Ph.D.

Chief Security Architect

DeepShield Systems, Inc.

Patent Attorney of Record:

Marcus Weber

European Patent Attorney

Registration No. EP12345