Zero-Day Attack Prevention Method Patent EP3967123

European Patent Specification

Patent Number: EP3967123

Filing Date: March 15, 2021

Publication Date: September 21, 2022

Patent Holder: DeepShield Systems, Inc.

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

Abstract

A method and system for preventing zero-day attacks in industrial control systems (ICS) and operational technology (OT) environments through real-time behavioral analysis and adaptive response mechanisms. The invention utilizes deep learning algorithms to establish baseline operational patterns and detect anomalous activities before they can exploit previously unknown vulnerabilities.

Technical Field

[0001] The present invention relates to cybersecurity systems for industrial control networks, specifically to methods for detecting and preventing zero-day attacks in operational technology environments through advanced machine learning and behavioral analysis.

Background

[0002] Industrial control systems face increasing threats from sophisticated cyber attacks, particularly zero-day exploits that target previously unknown vulnerabilities. Traditional signature-based detection methods prove inadequate against such novel threats.

[0003] Existing solutions typically rely on known attack patterns and fail to identify new attack vectors in real-time, leaving critical infrastructure vulnerable to emerging threats.

Summary of Invention

[0004] The present invention provides a novel method for zero-day attack prevention comprising:

a) A deep learning engine that continuously monitors network traffic and system behavior within ICS environments;

b) Real-time behavioral analysis algorithms that establish and maintain dynamic baseline operational patterns;

c) Anomaly detection mechanisms specifically calibrated for industrial protocols and operational patterns;

d) Automated response capabilities that can quarantine suspicious activities without disrupting critical operations.

Detailed Description

[0005] The invention implements a multi-layer detection and prevention architecture:

Layer 1: Data Collection and Analysis

[0006] Continuous monitoring of:

- Network traffic patterns
- Control system commands
- Process variables
- Operational states
- System configurations

Layer 2: Behavioral Modeling

[0007] Implementation of:

- Dynamic baseline generation
- Pattern recognition algorithms
- Deviation analysis
- Context-aware correlation

Layer 3: Threat Detection

[0008] Utilization of:

- Machine learning classifiers
- Statistical analysis engines
- Behavioral anomaly detection
- Protocol validation checks

Layer 4: Response Mechanism

[0009] Execution of:

- Automated threat containment
- Selective traffic filtering
- System state preservation
- Incident response workflows

Claims

A method for preventing zero-day attacks in industrial control systems comprising:

a) Monitoring real-time network traffic and system behavior;

b) Establishing dynamic behavioral baselines through machine learning;

c) Detecting anomalous activities through multi-factor analysis;

d) Implementing automated response mechanisms.

The method of claim 1, wherein behavioral baselines are continuously updated using deep learning algorithms.

The method of claim 1, wherein anomaly detection incorporates industrial protocol-specific validation.

Technical Implementation

[0010] The invention is implemented through:

- Distributed monitoring agents
- Centralized analysis engine
- Neural network processors
- Secure communication channels
- Automated response modules

Industrial Applicability

[0011] The invention is particularly applicable to:

- Manufacturing facilities
- Power generation plants
- Maritime infrastructure
- Oil and gas operations
- Critical infrastructure systems

Legal Notices

[0012] This patent document contains proprietary information of DeepShield Systems, Inc. All rights reserved. Any unauthorized copying, modification, or distribution is strictly prohibited.

Patent History

Priority Date: March 15, 2021

PCT Application: PCT/US2021/022831

Regional Phase Entry: September 15, 2021

Grant Date: September 21, 2022

Assignee Information

DeepShield Systems, Inc.
1234 Innovation Drive
Wilmington, Delaware 19801
United States of America

Patent Representatives

Smith & Associates LLP
Patent Registration No. 12345
Washington, DC

End of Patent Document EP3967123