TECHNISCHE HOCHSCHULE DEGGENDORF
Technologie Campus Vilshofen

CAIDAN

ELEVATING INDUSTRIAL CYBERSECURITY WITH AI-INTEGRATED HYBRID INTRUSION DETECTION SYSTEM FOR REAL-TIME CYBERATTACK ATTRIBUTION, ENHANCING INFRASTRUCTURE SECURITY, AND ENHANCED SITUATIONAL AWARENESS.

CAIDAN

Bundesministerium
für Bildung
und Forschung

Weitere Infos

Abstract

Projekttitel/ Project title:

Cyberattack Attribution Using AI-Enhanced Intrusion Detection with alert Correlation in Industrial Networks.

Kurztitel/ Short title:

CAIDAN

Einleitung/ Introduction:

In the ever-evolving landscape of industrial cybersecurity, attributing cyberattacks remains a critical challenge. The lack of adaptability in classic Intrusion Detection Systems (IDS), coupled with high error rates from contextless anomaly detection, and the absence of standardized forensic interfaces hinder effective response. This research addresses these challenges by proposing an AI-enhanced approach for cyberattack attribution in industrial networks. As industries become more connected, the vulnerabilities of Small and Medium Enterprises (SMEs) underscore the urgent need for advanced and accessible security measures.

Ziel/ Aim:

The aim of this research is to revolutionize industrial cybersecurity by integrating AI into intrusion detection systems. Our objective is to achieve real-time, accurate attribution of cyberattacks, enhancing situational awareness and mitigating operational risks. By addressing challenges posed by network complexity and SME vulnerabilities, we aim to create a scalable, transparent, and effective framework. Key innovations include a hybrid anomaly detection system based on data context, a correlation framework for precise alerts, and standardized forensic readiness. This research strives for resource-efficient, timely cyber-attack detection, indisputable attribution, and improved infrastructure security.

Methode/ Method:

The research methodology encompasses five work packages to systematically address the challenges of cyberattack attribution in industrial networks. Work Package 1 involves a comprehensive analysis of existing systems, refining use cases, and defining requirements and interfaces for the AI-Enhanced Intrusion Detection and Attribution Network. In Work Package 2, we design and implement a hybrid Intrusion Detection System (IDS), merging signature and anomaly-based approaches, incorporating AI-supported anomaly detection, and conducting thorough functional and integration tests. Work Package 3 focuses on a real-time alert correlation framework, specifying temporal dependencies for long-term analysis, and evaluating the developed framework. Work Package 4 conducts a forensic interface analysis, identifying connections and implementing universally applicable forensic measures. Finally, Work Package 5 integrates all components, conducts comprehensive testing, evaluates detection quality, and explores potential applications in diverse industrial contexts. This structured approach ensures the development of an effective, adaptive, and scalable solution for cyberattack attribution in industrial networks.

Ergebnis/ Result:

The result will showcase the successful development and integration of an AI-Enhanced Intrusion Detection and Attribution Network. Through comprehensive testing, CAIDAN will demonstrate real-time, accurate cyberattack attribution, enhanced situational awareness, and improved infrastructure security in diverse industrial networks, validating its effectiveness and adaptability.

Projektbeteiligte/ Project participants:

Prof. Dr. Michael Heigl, Andreas Urmann, Santhosh Kumar Nataraj

Projektpartner/ Project partners:

Technische Hochschule Deggendorf, TG Alpha GmbH, Trufflepig IT-Forensics GmbH TF, CIM GmbH, AVS Römer GmbH & Co. KG, Universität Augsburg

Gefördert durch/ Funded by:

Bundesministerium für Bildung und Forschung (BMBF)

Logos/ Logos:

CAIDAN

TECHNISCHE HOCHSCHULE DEGGENDORF
Technologie Campus Vilshofen

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

CIM LOGISTICS SOFTWARE SPECIALISTS

TRUFFLEPIG FORENSICS

TG α