Artificial Intelligence for Cybersecurity: Towards Taxonomy-based Archetypes and Decision Support

Completed Research Paper

Jana Gerlach
Leibniz University Hannover
Königsworther Platz 1
30167 Hanover, Germany
gerlach@iwi.uni-hannover.de

Oliver Werth
Leibniz University Hannover
Königsworther Platz 1
30167 Hanover, Germany
werth@iwi.uni-hannover.de

Michael H. Breitner
Leibniz University Hannover
Königsworther Platz 1
30167 Hanover, Germany
breitner@iwi.uni-hannover.de

Abstract

Cybersecurity is a critical success factor for more resilient companies, organizations, and societies against cyberattacks. Artificial intelligence (AI)-driven cybersecurity solutions have the ability to detect and respond to cyber threats and attacks and other malicious activities. For this purpose, the most important resource is security-relevant data from networks, cloud systems, clients, e-mails, and previous cyberattacks. AI, the key technology, can automatically detect, for example, anomalies and malicious behavior. Consequently, the market for AI-driven cybersecurity solutions is growing significantly. We develop a taxonomy of AI-driven cybersecurity business models by classifying 229 real-world services. Building on that, we derive four specific archetypes using a cluster analysis toward a comprehensive academic knowledge base of business model elements. To reduce complexity and simplify the results of the taxonomy and archetypes, we propose DETRAICS, a decision tree for AI-driven cybersecurity services. Practitioners, decision-makers, and researchers benefit from DETRAICS to select the most suitable AI-driven service.

Keywords: Artificial intelligence, AI-driven cybersecurity, taxonomy, archetypes, decision tree

Introduction

Cyberspace is exposed to a variety of risks resulting from physical and cyber threats amplified by the progressing digital transformation among the most affecting technologies such as the internet of things, digital platforms, cloud computing, and artificial intelligence (AI) (CISA 2022; European Parliament 2022a). A growing volume, velocity, and variety of data is collected, processed, and transmitted in cyberspace which is by design interconnected with data from the digital and physical world, thus emerging new dangers in the form of cyberattacks (CISA 2022; ENISA 2022). According to the European Parliament (2022b), cyberattacks are "attempts to misuse information, by stealing, destroying or exposing it, aiming