THE IMPACT OF ARTIFICIAL INTELLIGENCE ON CYBER SECURITY

Navigating the double-edged sword of technology

March 2024

Executive Brief

Blue River Experts

Member of the **Art of Innovation** Network

1 Overview

In recent months we have witnessed the fascinating convergence of two key areas of information technology – Cyber Security and Artificial Intelligence (AI). We have seen that AI plays an important but also dual-edged role. AI can be used to support and improve defensive measures but also as a tool to facilitate cyber-attacks. This session explains the various flavors of artificial intelligence, why it is important for Cyber Security, and what defensive tasks and measures can be improved by using AI. We will also look at some practical examples and use cases. Then we will examine how AI can be used to support cyber-attacks and will have a look at several examples. The session closes with summarizing the dual-edged role of AI and a few recommendations that will help participants to determine next steps.

2 Target Audience

This session has been designed for executives like Chief Information Security Officers, Chief Information Officers, but also Chief Executive Officers, Chief Operations Officers, Board Members, and everyone in a managing role being responsible for the well-being of a company or organization.

3 Objectives

After attending this session, participants will have a solid understanding of how AI is revolutionizing Cyber Security, if and how AI can be successfully used in defending against cyber-attacks but also the various facets where AI is supporting cyber-attacks and is used to enhance cyber-threats.

4 Speaker

This executive brief has been designed and will be delivered by Eckhart Eichler, a senior technology, strategy, and business advisor with extensive experience in applying technology to enable innovation and sustainable business growth. Eckhart has worked in the IT industry in Europe and the US for more than 35 years including regional and global leadership positions in various companies including his own successful consulting and education company.

During his career, Eckhart has been chairman, speaker and instructor at many international events and has delivered a vast number of presentations, workshops, courses, and keynotes. Right now, Eckhart is CTO at an expert company focusing on advanced technologies like Cyber Security, Cloud, and IoT.

5 Content Details

During this 2-hour session we will cover the following:

- Artificial Intelligence Overview
  - What is Artificial Intelligence
  - AI flavors and categories
  - Neural Networks
- The Importance of Cyber Security
- The Impact of AI on Cyber Security
  - How to use AI in Cyber Security defense
    - Log Analysis, Threat Detection
    - Digital Forenciscs, Threat Hunting
    - Automated Incident Response
    - User Behavior Analytics
    - Malware Detection and Prevention
    - Code Review, Vulnerability Detection
  - Recent advancements and trends
  - Practical examples and use cases

- The Dark Side of AI
  - Enabling and Supporting Threat Actors
  - Examples of AI used in cyber-attacks
    - Advanced Phishing, Social Engineering
    - AI-Driven Malware Development
    - Automated Exploit Generation
    - AI-Controlled Botnets
    - Next Generation Ransomware
- Summary and Recommendations
    - Is AI required for cyber-defense?
    - What's the impact of AI supported attacks on critical infrastructure
    - How to keep up as an organization

During this session there is sufficient time for questions, discussions, and individual recommendations.

Ideally, this executive brief is delivered to the executive staff of one organization so that we can have a lively and open discussion about the situation and the challenges this organization is facing.

In such a case this executive brief can be extended with an afternoon or second session where we can run a workshop, identifying potential solutions and next steps.