US 20240214409A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2024/0214409 A1**

Zahavi et al. (43) **Pub. Date: Jun. 27, 2024**

(54) **SYSTEMS AND METHODS FOR USING MACHINE LEARNING MODELS FOR IMPROVED AND CUSTOMIZED CYBER THREAT INTELLIGENCE**

(71) Applicant: **COGNYTE TECHNOLOGIES ISRAEL LTD**, HERZLIYA PITUACH (IL)

(72) Inventors: **Gilad Zahavi**, Herzliya Pituach (IL); **MICKAEL SOUSSAN**, Herzliya Pituach (IL)

(21) Appl. No.: **18/395,855**

(22) Filed: **Dec. 26, 2023**

Related U.S. Application Data

(60) Provisional application No. 63/435,362, filed on Dec. 27, 2022.

Publication Classification

(51) **Int. Cl.**

H04L 9/40	(2006.01)
G06F 40/295	(2006.01)
G06F 40/40	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 63/1433*** (2013.01); ***G06F 40/295*** (2020.01); ***G06F 40/40*** (2020.01)

(57) **ABSTRACT**

The present disclosure provides a method and system to produce a custom threat actor score. Generic cyber threat intelligence (CTI) is received by the system and analyzed by a natural language processor to generate cyber-attack parameters. A generic score is calculated based on the cyber-attack parameters. New Data of Interest (NDI) is collected from an enterprise and processed through a machine learning model to generate analyzed NDI data terms. An NLP is updated with the analyzed NDI data terms to create an enhanced NLP engine. The enhanced NLP engine generates custom cyber-attack parameters from CTI sources. A custom threat score is calculated based on the cyber-attack parameters combined with the custom cyber-attack parameters.