

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
07 December 2023 (07.12.2023)



(10) International Publication Number
WO 2023/232794 A1

(51) International Patent Classification:

G06F 21/55 (2013.01) H04L 9/40 (2022.01)
G06F 21/57 (2013.01)

(21) International Application Number:

PCT/EP2023/064416

(22) International Filing Date:

30 May 2023 (30.05.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2207992.5 30 May 2022 (30.05.2022) GB
2214371.3 30 September 2022 (30.09.2022) GB

(71) Applicant: **SENSEON TECH LTD** [GB/GB]; 100 Pall Mall, London SW1Y 5NQ (GB).

(72) Inventors: **GEROW, Aaron**; 100 Pall Mall, London SW1Y 5NQ (GB). **MISTRY, James**; 100 Pall Mall, London SW1Y 5NQ (GB).

(74) Agent: **THOMAS DUNCAN WOODHOUSE**; PAGE WHITE & FARRER, Bedford House, John Street, London Greater London WC1N 2BF (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE

(54) Title: CYBERSECURITY THREAT DETECTION

(57) Abstract: A cybersecurity platform for detecting potential cybersecurity threats pertaining to a set of computer infrastructure, the cybersecurity platform comprising: event storage configured to receive and store multiple forms of telemetry pertaining to the set of computer infrastructure, in the form of structured telemetry events having a common data format, the multiple forms of telemetry having been processed into the structured telemetry events having the common data format based a plurality of predetermined telemetry data schemas; a threat detection component operable to receive a configuration input, the threat detection component configurable based on the configuration input to apply a plurality of signature-based detection rules to the multiple forms of telemetry, wherein each signature-based detection rule is defined in the configuration input and comprises: a reference to a target data field within the set of predetermined telemetry data schemas, and a target pattern indicative of a potential cybersecurity threat; wherein the threat detection component is configured to apply the plurality of signature-based detection rules by executing a pattern recognition algorithm, based on the target pattern, on the target data field of each structured telemetry event having the target data field, and cause a detection output to be generated based on detecting the target pattern in the target data field of a structured telemetry event.

WO 2023/232794 A1