



(51) International Patent Classification:
H04L 9/40 (2022.01) *G06F 21/57* (2013.01)
G06F 21/55 (2013.01)

(21) International Application Number:
PCT/US2023/030480

(22) International Filing Date:
17 August 2023 (17.08.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/398,611 17 August 2022 (17.08.2022) US

(71) Applicant: **BOOZ ALLEN HAMILTON INC.** [US/US];
8283 Greensboro Drive, McLean, Virginia 22102 (US).

(72) Inventors: **JILANI, Ammad**; 5701 Woodview Avenue,
Austin, Texas 78756 (US). **LIOTT, Jeffrey M.**; 16834
Granite Way, Milton, Delaware 19968 (US). **MAO,
Stephen Jy**; 13523 DaVinci Lane, Herndon, Virginia
20171 (US). **MCDANIEL, Steven Ryan**; 237 E. Sky
View Lane, Washington, Vermont 84780 (US). **MCCUL-
LOUGH, Gregory**; 12003 Uplands Ridge Drive, Austin,
Texas 78738 (US). **RAMAN, Arjun Gargi**; 6007 Sun Vista
Drive, Austin, Texas 78749 (US). **TANG, Eric Tsz Leung**;
11684 Fox Glen Drive, Oakton, Virginia 22124 (US).

(74) Agent: **KEANE, Patrick C.** et al.; Buchanan Ingersoll &
Rooney PC, 1737 King Street, Suite 500, Alexandria, Vir-
ginia 22314-2727 (US).

(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).

(54) Title: SYSTEM AND METHOD FOR RISK-BASED OBSERVABILITY OF A COMPUTING PLATFORM

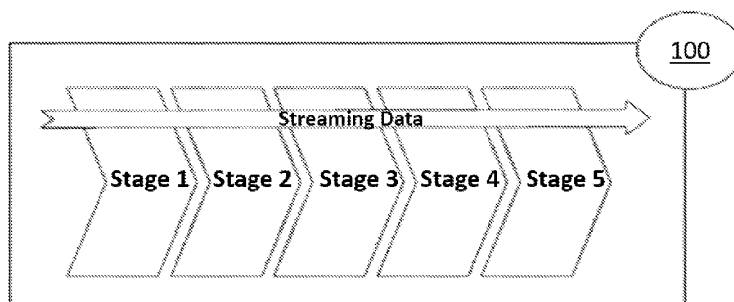


FIG. 1

(57) Abstract: Exemplary systems and methods are directed to risk-based observability of a platform. Data is received from plural devices from one or more computing environments on a network. The received data is in a raw data format according to the computing environment or platform from which it was received. The received data is converted from the raw format to a structured format. The converted data is enhanced by adding contextual information associated with a corresponding one of the plural devices. A risk analysis is performed on the enhanced data based on one or more risk detection rules applied to the network. One or more tags are applied to the enhanced data based on results of the risk analysis. Data analysis is performed on the enhanced data to identify devices from aggregate sources. The data is sent to one or more destinations on the network based on the applied tags.

[Continued on next page]

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:

28 March 2024 (28.03.2024)