



- (51) **International Patent Classification:**
H04L 29/06 (2006.01) *G06F 21/55* (2013.01)
- (21) **International Application Number:**
PCT/EP2020/058028
- (22) **International Filing Date:**
23 March 2020 (23.03.2020)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
16/387,632 18 April 2019 (18.04.2019) US
- (71) **Applicant:** **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, New York 10504 (US).
- (71) **Applicant (for MG only):** **IBM DEUTSCHLAND GMBH** [DE/DE]; c/o IBM Deutschland Management & Business Support GmbH, Patentwesen und Urheberrecht, IBM Allee 1, 71139 Ehningen (DE).
- (72) **Inventors:** **UDUPI RAGHAVENDRA, Arjun;** c/o IBM Switzerland AG, Vulkanstrasse 106, 8048 Zuerich (CH). **SEUL, Matthias;** c/o IBM Corp., 425 Market St, Floor 20, San Francisco, California 94105 (US). **SCHEIDELER, Tim;** c/o IBM Switzerland AG, Vulkanstrasse 106, 8048 Zuerich (CH). **AIROLDI, Tiziano;** c/o IBM Italia SpA, Via Fornace, 43, 20866 Carnate (IT).
- (74) **Agent:** **KLETT, Peter;** c/o IBM Deutschland Management & Business Support GmbH, Patentwesen und Urheberrecht, IBM Allee 1, 71139 Ehningen (DE).
- (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) **Title:** DETECTING SENSITIVE DATA EXPOSURE VIA LOGGING

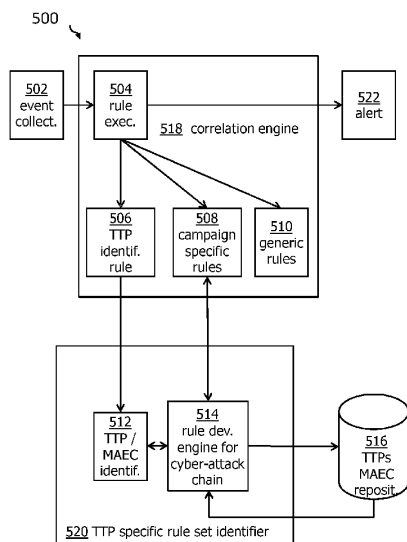


FIG. 5

(57) **Abstract:** A computer-implemented method for dynamically identifying security threats comprising a cyber-attack chain composed of a sequence of partial cyber-attacks represented by attack patterns is provided. The method comprises receiving a sequence of security events, determining, a first cyber-attack pattern by applying a set of predefined rules for detecting an indicator of compromise of a first partial cyber-attack of the cyber-attack chain – thereby, identifying a specific cyber-attack chain – and determining a type and an attribute in the pattern of the first partial cyber-attack. The method comprises further configuring at least one rule for a downstream partial cyber-attack in the specific cyber-attack chain based on the type and the attribute in the attack pattern of the first partial cyber-attack, and adding the at least one configured rule to the set of predefined rules to be used by the correlation engine for dynamically identifying security threats.

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))*