



(51) International Patent Classification:

H04L 29/06 (2006.01) H04L 29/12 (2006.01)
H04W 12/12 (2009.01)

(21) International Application Number:

PCT/EP2019/070256

(22) International Filing Date:

26 July 2019 (26.07.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

1812171.5 26 July 2018 (26.07.2018) GB

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

(72) Inventors: ATKINSON, David; C/O Senseon Tech Ltd, 100 Pall Mall, London SW1Y 5NQ (GB). MISTRY, James; C/O Senseon Tech Ltd, 100 Pall Mall, London SW1Y 5NQ (GB).

(74) Agent: THOMAS DUNCAN WOODHOUSE et al.; 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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, 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))

(54) Title: CYBER DEFENCE SYSTEM

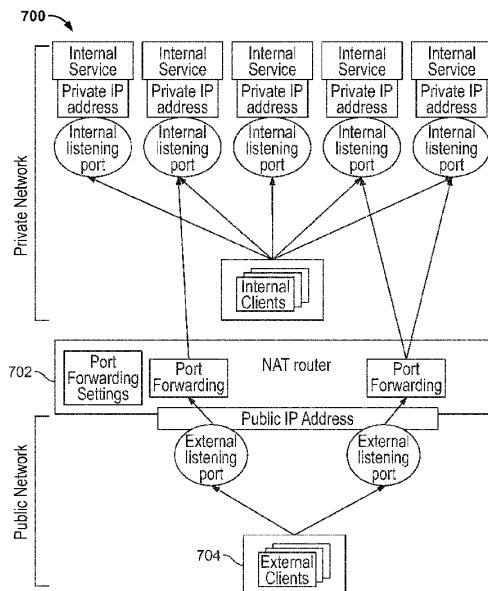


Figure 6

(57) Abstract: A method of detecting security threats comprises: in an enrichment stage, receiving events pertaining to a monitored private network; enriching the events by augmenting them with enrichment data; and receiving, at an analysis engine, the enriched events and analysing the enriched events to detect security threat conditions indicated by the enriched events; wherein at least one of the events is enriched based on external reconnaissance by: determining a related public network address on a network interface between the private network and a public network, and augmenting the event with external reconnaissance data, as determined by transmitting at least one reconnaissance message from an external reconnaissance device on the public network to the related public network address on the network interface between the public and the private networks.