

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

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
24 November 2011 (24.11.2011)

(10) International Publication Number  
**WO 2011/146284 A2**

PCT

(51) International Patent Classification:  
**G05B 9/02** (2006.01) **G06F 1/26** (2006.01)

(21) International Application Number:  
PCT/US2011/035888

(22) International Filing Date:  
10 May 2011 (10.05.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
61/346,787 20 May 2010 (20.05.2010) US

(71) Applicant (for all designated States except US): **AC-CENTURE GLOBAL SERVICES LIMITED** [IE/IE];  
3 Grand Canal Plaza, Grand Canal Street Upper, Dublin,  
4 (IE).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **SCOTT, Anthony, David** [US/US]; 1022 Otis Street, Washington, DC 20017 (US).

(74) Agent: **GREENE, Nathan, O.**; Brinks Hofer Gilson & Lione, P.O. Box 10087, Chicago, IL 60610 (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: MALICIOUS ATTACK DETECTION AND ANALYSIS

(57) Abstract: A system for characterizing malicious activity in an intelligent utility grid system includes a system storage in which to store a database including a plurality of rules. A collector is operable to collect and store in the system storage information-technology (IT) data including IT-related activity from the intelligent grid system. A complex event processing (CEP) bus is operable to receive non-IT data including location-specific event data from a plurality of electronic sources, the CEP bus further operable to disregard the non-IT data failing to meet a predetermined level of relevance to one of a plurality of risk-related events. A processor is operable to apply the plurality of rules to the relevant non-IT data to: associate an undesired event with reference to the IT-related activity; and determine a probability that the undesired event is indicative of malicious activity. The processor further applies a risk characterization to the undesired event based on the probability and the IT-related activity.



WO 2011/146284 A2