



- (51) **International Patent Classification:**
G06F 21/50 (2013.01) *G06F 11/30* (2006.01)
- (21) **International Application Number:**
PCT/US2013/075856
- (22) **International Filing Date:**
17 December 2013 (17.12.2013)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/728,746 27 December 2012 (27.12.2012) US
- (71) **Applicant:** CROWDSTRIKE, INC. [US/US]; 30251 Golden Lantern, Laguna Niguel, CA 92677-5993 (US).
- (72) **Inventor:** DIEHL, David, F.; 5324 Elliot Ave S, Minneapolis, MN 55417 (US).
- (74) **Agents:** PECK, Robert, C. et al.; Lee & Hayes, PLLC, 601 W. Riverside Ave, Suite 1400, Spokane, WA 99201 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, 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, 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).

[Continued on next page]

(54) **Title:** REAL-TIME REPRESENTATION OF SECURITY-RELEVANT SYSTEM STATE

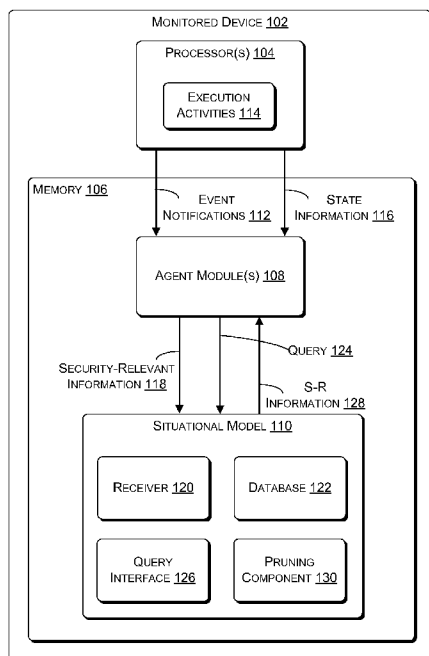


Fig. 1

(57) **Abstract:** A situational model representing of a state of a monitored device is described herein. The situational model is constructed with the security-relevant information in substantially real-time as execution activities of the monitored device associated with the security-relevant information are observed. The represented state may include a current state and a past state of the monitored device. Also, the situational model may be used to validate state information associated events occurring on the monitored device. Further, a remote security service may configure the monitored device, including configuring the situational model, and may build an additional situational model representing a state of a group of monitored devices.



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))