

(51) International Patent Classification:
G06F 11/00 (2006.01)(21) International Application Number:
PCT/US2015/056082(22) International Filing Date:
16 October 2015 (16.10.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/066,769 21 October 2014 (21.10.2014) US(71) Applicant: **IRONNET CYBERSECURITY, INC.**
[US/US]; 8135 Maple Lawn Blvd., Suite 455, Fulton, MD 20759 (US).(72) Inventors: **GROSSMAN, Robert, L.**; 435 Jackson Ave., River Forest, IL 60305 (US). **HEATH, James, E.**; 17034 Kingfish Ln. W., Sugar Loaf Key, FL 33042 (US). **RICHARDSON, Russell, D.**; 8408 Sparger Street, McLean, VA 22101 (US). **ALEXANDER, Keith, B.**; 8135 Maple Lawn Blvd., Suite 455, Fulton, MD 20759 (US).(74) Agents: **STEINBERG, Donald, R.** et al.; Wilmer Cutler Pickering Hale and Dorr LLP, 60 State Street, Boston, MA 02109 (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, 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))

[Continued on next page]

(54) Title: CYBERSECURITY SYSTEM

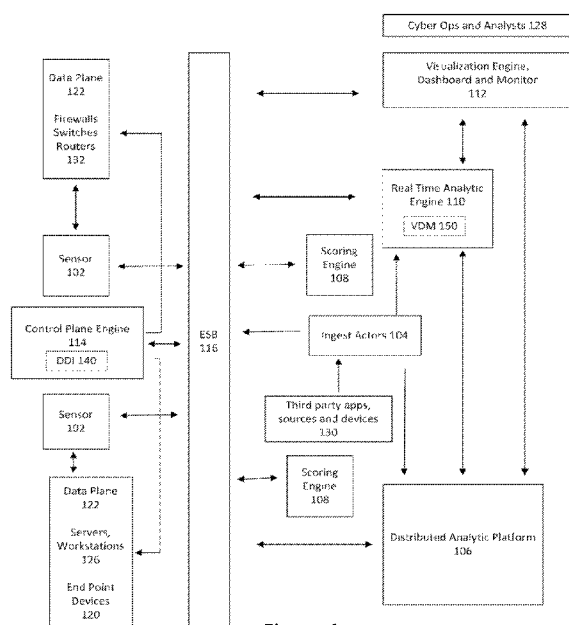


Figure 1

(57) Abstract: A cybersecurity system for processing events to produce scores, alerts, and mitigation actions. The system includes sensors for receiving and processing data to form events, distributed analytic platform for processing events to form analytic workflows, and scoring engines for processing events using analytic workflows to produce scoring engine messages. The system also includes real time analytic engine for processing scoring engine messages and distributed analytic platform messages using the analytic workflows and analytic workflow and event processing rules to form and transmit a threat intelligence message. Threat intelligence messages include broadcast messages, mitigation messages, and model update messages. The system also includes logical segments which associate an analytic model, a set of analytic models, or an analytic workflow; one or more sources of inputs about activity within the logical segment, and a set of actions for mitigating an impact of the anomalous activity occurring within the logical segment.



— *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:**
9 September 2016