(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 5 月 16 日 (16.05.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/098699 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01)

(21) 国际申请号: PCT/CN2023/093384

(22) 国际申请日: 2023 年 5 月 11 日 (11.05.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202211412683.2 2022年11月11日 (11.11.2022) CN

(71) 申请人:上海派拉软件股份有限公司(**SHANGHAI PARAVIEW SOFTWARE CO., LTD**) [CN/CN]; 中国上海市浦东新区中国（上海）自由贸易试验区龙东大道3000号1幢裙楼208室, Shanghai 201203 (CN)。

(72) 发明人:徐莉莎(**XU, Lisha**); 中国上海市浦东新区中国（上海）自由贸易试验区龙东大道3000号1幢裙楼208室, Shanghai 201203 (CN)。 陈远猷(**CHEN, Yuanyou**); 中国上海市浦东新区中国（上海）自由贸易试验区龙东大道3000号1幢裙楼208室, Shanghai 201203 (CN)。

(74) 代理人:北京品源专利代理有限公司(**BEYOND ATTORNEYS AT LAW**); 中国北京市海淀区莲花池东路39号西金大厦6层, Beijing 100036 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE,

(54) **Title:** ENTITY OBJECT THREAD DETECTION METHOD AND APPARATUS, DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 实体对象的威胁检测方法、装置、设备及存储介质

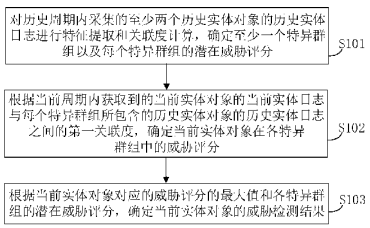


图 1

S101 Perform feature extraction and degree of correlation calculation on the historical entity logs of at least two historical entity objects collected within a historical period, and determine at least one specific group and a potential threat score for each specific group

S102 According to a first degree of correlation between a current entity log of a current entity object obtained in the current period and a historical entity log of a historical entity object contained in each specific group, determine a threat score for a current entity object in each specific group

S103 According to the highest threat score corresponding to the current entity object and the potential threat score of each specific group, determine a threat detection result for the current entity object

(57) **Abstract:** The present application discloses an entity object threat detection method and apparatus, a device, and a storage medium. The method comprises: performing feature extraction and degree of correlation calculation on the historical entity logs of at least two historical entity objects collected within a historical period, and determining at least one specific group and a potential threat score for each specific group; according to a first degree of correlation between a current entity log obtained in the current period and each historical entity log contained in each specific group, determining a threat score for a current entity object in each specific group; and according to the highest threat score corresponding to the current entity object and the potential threat score of each specific group, determining a threat detection result for the current entity object.

(57) 摘要: 本申请公开了一种实体对象的威胁检测方法、装置、设备及存储介质，该方法包括：对历史周期内采集的至少两个历史实体对象的历史实体日志进行特征提取和关联度计算，确定至少一个特异群组以及每个特异群组的潜在威胁评分；根据当前周期内获取到的当前实体日志与每个特异群组所包含的历史实体日志之间的第一关联度，确定当前实体对象在各特异群组中的威胁评分；根据所述当前实体对象对应的威胁评分的最大值和各所述特异群组的潜在威胁评分，确定所述当前实体对象的威胁检测结果。

WO 2024/098699 A1

[见续页]

BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。