实体对象的威胁检测方法、装置、设备及存储介质

本公开要求在2022年11月11日提交中国专利局、申请号为202211412683.2的中国专利申请的优先权，该申请的全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机技术领域，例如涉及一种实体对象的威胁检测方法、装置、设备及存储介质。

背景技术

网络技术的进步和信息化的普及，给各个产业带来了新的发展机遇，同时也带来了网络安全威胁。网络系统由于内部系统的脆弱性或者被恶意攻击而发生信息泄露，数据破坏，资源非法使用、越权等威胁，会对企业造成极大的损失。现有的攻击案例显示，大部分正常用户访问网络资源的模式是存在用户自身特征的，相似程度较低，而网络攻击是群组攻击，这些群组对象强相似、紧耦合。

相关技术的威胁检测方法主要包括两类，一类是通过安全专家经验检测各类风险模式，并根据自定义权重对各类风险进行评分。这种方式过度依赖专家经验，人力成本高，且自定义权重不适用于日益变化的威胁。另一类是通过机器学习的方式，采用监督式分类方法检测已知的各类风险，然后根据概率获得评分。这种方式要求训练数据具有良好的特征和准确的标签，需要标注人员具有专业的网络安全知识，标注成本较高，在应对未知的威胁时，检测和评分结果易造成较大误差。

发明内容

本申请提供了一种实体对象的威胁检测方法、装置、设备及存储介质，实现无监督的威胁检测方法，有效降低了威胁检测成本，提高了对威胁评分判断的准确性，有效保证了实体对象威胁可参考的全面性。

第一方面，本公开实施例提供了一种实体对象的威胁检测方法，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对象的当前实体日志与每个特异群组所包含的历史实体对象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。

第二方面，本公开实施例提供了一种实体对象的威胁检测装置，包括：

历史威胁评分模块，设置为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；

当前威胁评分模块，设置为根据当前周期内获取到的当前实体对象的当前实体日志与每个特异群组所包含的历史实体对象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；

检测结果确定模块，设置为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。

第三方面，本公开实施例提供了一种电子设备，包括：

至少一个处理器；以及

与至少一个处理器通信连接的存储器；其中，

存储器存储有可被至少一个处理器执行的计算机程序，计算机程序被至少一个处理器执行，以使至少一个处理器能够执行上述第一方面实施例提供的实体对象的威胁检测方法。

第四方面，本公开实施例提供了一种计算机可读存储介质，计算机可读存储介质存储有计算机指令，计算机指令用于使处理器执行时实现上述第一方面实施例提供的实体对象的威胁检测方法。

本申请实施例提供的一种实体对象的威胁检测方法、装置、设备及存储介质，通过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对象的当前实体日志与每个特异群组所包含的历史实体对象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；根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果。通过采用上述技术方案，采集历史实体对象横向维度以及时间维度的实体日志，聚合具体实体多个阶段、多个场景的习惯对实体进行特征构建，使实体画像更加具体；根据攻击的少数

相似性，构建特异群组并进行分析的方法，更贴近实际攻击的特征。上述技术方案，有效降低了威胁检测成本，提高了对威胁评分判断的准确性，保证了实体对象威胁可参考的全面性。

附图说明

为了说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作介绍，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例一提供的一种实体对象的威胁检测方法的流程图；

图 2 是本申请实施例二提供的一种实体对象的威胁检测方法的流程图；

图 3 是本申请实施例二所提供一种实体对象的威胁检测方法的架构示意图；

图 4 是本申请实施例三提供的一种实体对象的威胁检测装置的结构示意图；

图 5 是本申请实施例四提供的一种电子设备的结构示意图。

具体实施方式

为了使本技术领域的人员理解本申请方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述，所描述的实施例仅仅是本申请一部分的实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“目标”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于列出的那些步骤或单元，而是可包括没有列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

实施例一

图 1 是本申请实施例一提供的一种实体对象的威胁检测方法的流程图，本实施例可适用于多种应用场景下对网络实体对象进行威胁检测的情形，该方法

可以由实体对象的威胁检测装置来执行，该实体对象的威胁检测装置可以采用硬件和/或软件的形式实现。

如图 1 所示，该方法包括：

S101、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。

在本实施例中，历史周期可以理解为历史时间内固定的时间间隔，该历史周期可以根据实际需求设定，例如可以是过去一周、过去两周或过去一个月等。历史实体对象可以理解为历史周期内采集到的能够标识用户的元素，例如可以包括账号、设备或网际协议（Internet Protocol，IP）等。历史实体日志可以理解为每一个历史实体对象的网络操作所形成的日志。

特异群组可以理解为基于关联度所确定的存在潜在威胁的实体所构成的群组，特异群组包括至少一个存在潜在威胁的实体对象。本申请实施例中特异群组的数量和特异群组中所含的实体对象的数量均可以根据实际需求设定。潜在威胁评分可以理解为历史实体对象的潜在威胁程度的评分。示例性的，获取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，并对每一个历史实体对象进行特征提取；根据提取到的特征构建特征矩阵，基于各历史实体对象的特征矩阵计算历史实体对象之间的关联度；根据历史实体对象之间的关联度确定至少一个特异群组；最终根据特异群组所包含的历史实体对象之间的关联度确定特异群组的潜在威胁程度评分。

示例性的，对历史实体日志进行特征提取的方式可以为将实体日志进行预处理，按照横向维度和时间序列维度聚合得到多元异构特征。对历史实体日志所包含特征可以包括最近一次登录的环境设备比例、是否常用时间登录、固定周期内登录的数量、访问时长、访问应用数量、访问应用顺序、下载文件的数量、修改文件的数量和操作的时间间隔等；提取历史实体日志 m 个特征，得到 m 维特征向量所构成特征矩阵。历史实体对象之间的关联度可以采用相似度或者一致度等进行计算，例如可以采用如余弦相似度、结构相似度、直方图等一系列可对比指标进行关联度计算。

示例性的，根据各历史实体对象之间的关联度确定至少一个特异群组的方式可以为：根据各历史实体对象之间的关联度进行基于关联度的挖掘算法或者最大团算法等算法群组挖掘确定至少一个特异群组。

S102、根据当前周期内获取到的当前实体对象的当前实体日志与每个特异群组所包含的历史实体对象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。

在本实施例中，当前周期可以理解为当前时间内固定的时间间隔，例如可以是一周、两周或一个月等。当前实体对象可以理解为当前周期内采集到的能够标识用户的元素，例如可以至少包括账号、设备、IP 等。需要说明的是，当前实体对象的数量可以是一个、两个或多个。当前实体日志可以理解为每一个历史实体对象的网络操作所形成的日志。可以理解的是，在本申请实施例中当前实体对象即为待威胁检测的实体对象。第一关联度可以理解为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关联度，也可以理解为当前实体对象与特异群组中的历史实体对象之间的关联度。

示例性的，在当前周期内获取当前实体对象的当前实体日志，并对当前实体日志进行特征提取得到当前实体对象所对应的特征矩阵；将当前实体对象的特征矩阵与每个特异群组所包含的各历史实体对象的特征矩阵进行关联度计算，确定当前实体对象与每个特异群组所包含的各历史实体对象之间的第一关联度；并确定当前实体对象在各特异群组中的威胁评分。其中，由于网络攻击是群组攻击，这些群组的实体对象之间具有较强的相似性与紧密的耦合关系，因此各实体对象之间关联度越高，存在的网络威胁越大。在本实施例中可以体现为，当前实体对象与特异群组中的各历史实体对象之间的第一关联度越高，当前实体对象的威胁评分越高。

需要说明的是，随着时间的推移，当前实体对象的当前实体日志也会变为历史实体对象的历史实体日志，参与到特异群组的潜在威胁评分的学习过程中，从而使特异群组的潜在威胁评分随着历史实体日志的更新不断得到学习，进而使得威胁实体群组能够更加切合实际的网络系统，提高威胁检测的准确性。

S103、根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果。

在本实施例中，当前实体对象的威胁检测结果可以理解为当前实体对象是否存在网络威胁的检测结果。当前实体对象存在对应的威胁评分，即当前实体对象在各特异群组中的威胁评分。

示例性的，确定当前实体对象在各特异群组中的威胁评分的最大值，将该最大值与每个特异群组的潜在威胁评分进行比较，根据比较的结果大小确定当前实体对象是否存在网络威胁。

示例性的，根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果的方式，可以为判断当前实体对象对应的威胁评分的最大值是否小于所有特异群组的潜在威胁评分；若是，

则确定当前实体对象不存在威胁；若否，则确定当前实体对象存在威胁。或者还可以为判断当前实体对象对应的威胁评分的最大值是否大于所有特异群组的潜在威胁评分；若是，则确定当前实体对象存在威胁；若否，则确定当前实体对象不存在威胁。

在本实施例中，通过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对象的当前实体日志与每个特异群组所包含的历史实体对象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；根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果。通过采用上述技术方案，采集历史实体对象横向维度以及时间维度的实体日志，聚合具体实体多个阶段、多个场景的习惯对实体进行特征构建，使实体画像更加具体；根据攻击的少数相似性，构建特异群组并进行分析的方法，更贴近实际攻击的特征。上述技术方案，有效降低了威胁检测成本，提高了对威胁评分判断的准确性，保证了实体对象威胁可参考的全面性。

可选的，该方法还包括：

若根据所述历史实体对象的历史实体日志确定不存在特异群组，则根据当前周期内获取到的当前实体对象的当前实体日志进行特征提取和关联度计算，确定是否存在特异群组；

若存在，则确定所述特异群组内的当前实体对象存在威胁；

若不存在，则确定所述当前实体对象不存在威胁。

示例性的，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，确定是否存在至少一个特异群组；若存在，则采用步骤S101～S103提供的实体对象的威胁检测方法确定当前周期内获取到的当前实体对象的威胁检测结果；若不存在，则无法按照步骤S103的方法“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”，此时需要根据当前周期内获取到的当前实体对象的当前实体日志进行特征提取和关联度计算，确定是否存在特异群组。若不存在特异群组，表示当前实体对象不存在威胁，若存在至少一个特异群组，则认为特异群组内的当前实体对象存在威胁，从而得到当前实体对象的威胁检测结果。

实施例二

图 2 是本申请实施例二提供的一种实体对象的威胁检测方法的流程图，本实施例是对上述任一实施例的优化，本实施例可适用于多种应用场景下对网络实体对象进行威胁检测的情形，该方法可以由实体对象的威胁检测装置来执行，该实体对象的威胁检测装置可以采用硬件和/或软件的形式实现。

如图 2 所示，该方法包括：

S201、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，得到各历史实体对象的第一特征矩阵。

在本实施例中，第一特征矩阵可以理解为历史实体对象的历史实体日志的多维特征向量所构成的特征矩阵。

可选的，步骤 S201 可以包括：

（1）获取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。

在历史周期时间内，采集至少两个历史实体对象所对应的记录注册、登录、访问应用、应用内操作的历史实体日志。

（2）对于每个历史实体对象对应的历史实体日志的日志信息，基于会话标记进行会话切分得到至少一个完整会话。

在本实施例中，每个历史实体对象对应的历史实体日志内存在日志信息，日志信息可以理解为会话信息的集合。其中，历史实体日志中可以基于时间维度包含至少一个完整的会话。会话是指实体对象在网络系统内访问网络资源的行为，例如登录、访问、信息下载和信息修改等，每一个完整的会话都可以存在一个唯一的会话标记。若存在多个会话，可以基于唯一的会话标记将多个会话进行切分，得到至少一个包含实体对象在网络系统内访问网络资源行为的完整会话。

（3）对于各所述完整会话，提取所述完整会话在预设维度特征参数上的特征得到所述完整会话的特征向量。

在本实施例中，预设维度特征参数可以理解为预设数量个不同维度的特征参数信息。

示例性的，将每一个完整会话的数据计算成一条向量特征，在会话内提取特征参数对应的 m 维特征向量，例如可以包括最近一次登录的环境设备比例、是否常用时间登录、固定周期内登录的数量、访问时长，访问应用数量，访问应用顺序，下载文件的数量，修改文件的数量，操作的时间间隔等 m 个特征信息，得到 m 维向量。

（4）对于各所述历史实体对象，根据所述历史实体对象对应的各所述完整

会话的特征向量按照会话发生时间排列得到初始特征矩阵。

在本实施例中，初始特征矩阵可以理解为针对历史实体对象对应的多维向量特征构建的初始矩阵。

示例性的，历史实体对象在历史周期内存在的所有会话按时间顺序排列为 r 个，并基于每一个会话存在的 m 维向量，按每一个会话的时间发生顺序，对历史周期内的所有会话分别计算向量特征，排列得到 r*m 形式的特征矩阵。计算所有历史实体对象的特征矩阵，例如存在 n 个历史实体对象，可以得到 n 个历史实体对象的矩阵分别为 r_1*m，r_2*m，…，r_n*m，此时将上述 n 个历史实体对象的特征矩阵确定为初始特征矩阵。

（5）对各所述初始特征矩阵进行平均池化得到各所述历史实体对象的第一特征矩阵。

在本实施例中，第一特征矩阵可以理解为对每个初始特征矩阵经平均池化后的特征矩阵。平均池化是神经网络中减少特征图大小，减少计算量和所需显存的方法，平均池化可以理解为对特征点只求平均特征，统一每个历史实体对象的特征维度的一种方法。

示例性的，利用平均池化的方式统一不同历史实体对象的矩阵特征维度，将初始特征矩阵 r_1*m，r_2*m，…，r_n*m 平均池化为第一特征矩阵 r_r*m。其中输出维度 r_r 可根据实际场景数据调整。

S202、对于每个包含两个历史实体对象的历史实体对象组，根据历史实体对象组的第一特征矩阵之间的关联度确定历史实体对象组的第二关联度。

在本实施例中，历史实体对象组可以理解为任意两个历史实体对象的集合。在历史实体对象组内，每个历史实体对象存在对应的第一特征矩阵。第二关联度可以理解为历史实体对象组内两个历史实体对象对应的第一特征矩阵之间的关联度。

示例性的，在历史实体对象组中包含两个不同的历史实体对象，每两个历史实体对象组内包含的历史实体对象也可以是不完全相同的，将历史实体对象组内两个历史实体对象的第一特征矩阵之间的关联程度，确定为第二关联度。

示例性的，历史实体对象组 A 内包含历史实体对象 1 与历史实体对象 2，两个历史实体对象分别对应第一特征矩阵 N1 与 N2，将 N1 与 N2 之间的关联度确定为历史实体对象 1 与历史实体对象 2 之间的关联度，即历史实体对象组 A 对应的第二关联度；历史实体对象组 B 内包含历史实体对象 3 与历史实体对象 4。其中，历史实体对象组 A 与历史实体对象组 B 可以是历史实体对象不完全相同的历史实体对象组。例如在历史实体对象组 A 内包含的历史实体对象 1 与历史

实体对象组 B 内包含的历史实体对象 3 可以是同一个历史实体对象。

S203、根据各历史实体对象组的第二关联度确定至少一个特异群组。

在本实施例中，每个历史实体对象组之间都存在对应的第二关联度，对每个历史实体对象组中第二关联度满足预设条件的历史实体对象进行基于关联度的群组挖掘，确定至少一个特异群组。

可选的，步骤 S203 可以包括：

（1）根据各所述历史实体对象组的第二关联度的排序，确定由第二关联度最大的第一预设数量的历史实体对象组构成的实体关联集合。

在本实施例中，第一预设数量可以理解为预设的实体关联集合的元素数量。实体关联集合可以理解为由预设数量的历史实体对象组所构成的集合。

示例性的，对各个历史实体对象组进行关联度由高到低的排序，根据最大关联度的排序，去除关联度较低的数据，取第二关联度中的前 k 名个历史实体对象组，将 k 个历史实体对象组的集合确定为实体关联集合，此时实体关联集合内存在 t 个历史实体对象（t<=2k）。实体关联集合中的历史实体对象数量 t 可以根据实际情况设置。其中 k 与 t 的关系可以是 kmax=t*(t-1)/2。

示例性的，若 k 为 3，且存在 4 个历史实体对象组，分别为历史实体对象组 A、B、C 和 D；其中，历史实体对象组 A 的第二关联度为 0.7，历史实体对象组 B 的第二关联度为 0.6，历史实体对象组 C 的第二关联度为 0.2，历史实体对象组 D 的第二关联度为 0.8。根据第二关联度从大至小进行排序，可以确定历史实体对象组 A、历史实体对象组 B 与历史实体对象组 D 的第二关联度排序为前三名，因此根据历史实体对象组 A、历史实体对象组 B 与历史实体对象组 D 的集合确定实体关联集合。

（2）对所述实体关联集合所包含的每个所述历史实体对象，将所述历史实体对象所属的历史实体对象组的第二关联度的最大值确定为所述历史实体对象的目标关联度。

在本实施例中，目标关联度可以理解为历史实体对象自身对应的关联度，例如可以将取最大值的第二关联度作为历史实体对象的目标关联度。

示例性的，实体关联集合中包含第一预设数量 k 个的历史实体对象组，其中第一预设数量的 k 个历史实体对象组包含 t 个历史实体对象，取实体关联集合中第一预设数量的各历史实体对象组的第二关联度，将 t 个历史实体对象所属的历史实体对象组所存在的第一预设数量个的第二关联度取最大关联度值，并将关联度最大的第二关联度确定为目标关联度。此实体关联集合内的历史实体对象满足：实体关联集合内的任意一个历史实体对象组 P，至少存在一个历史实体

对象组 Q 使得 similarity(P，Q)>=min(实体关联集合中所有历史实体对象组的第二关联度)。Q 可以理解为目标关联度所对应的历史实体对象组。

示例性的，若 t=5，k=7，存在 5 个历史实体对象 1-5，以及五个历史实体对象对应的 7 个历史实体对象组。例如包括（1，2）、（1，3）、（1，4）、（2，3）、（2，5）、（3，4）与（4，5）。此时历史实体对象 1 对应的历史实体对象组包括（1，2）、（1，3）与（1，4），其中，三个历史实体对象组对应的第二关联度分别为 0.7、0.6 与 0.3，此时确定（1，2）对应的第二关联度 0.7 为历史实体对象 1 的目标关联度。历史实体对象 2 对应的历史实体对象组包括(2，3）与（2，5），其中，两个历史实体对象组对应的第二关联度分别为 0.5、与 0.9，此时确定（2，5）对应的第二关联度 0.9 为历史实体对象 2 的目标关联度。同理，由于历史实体对象 3、历史实体对象 4 与历史实体对象 5 在实体关联集合中都仅存在一个历史实体对象组，因此历史实体对象对应的唯一一个历史实体对象组的第二关联度可以直接被确定为目标关联度。此时，确定在实体关联集合中存在与历史实体对象数量相同的五个目标关联度。

（3）根据所述实体关联集合中各所述历史实体对象的目标关联度的排序，确定由目标关联度最大的第二预设数量的历史实体对象构成的候选特异集合。

在本实施例中，候选特异集合可以理解为由实体关联集合中目标关联度满足预设条件的历史实体对象所构成的实体集合，候选特异集合中的历史实体对象可以作为威胁实体群组的候选对象。实体关联集合中的历史实体对象满足的预设条件可以为：在目标关联度从大至小的排序中靠前的第二预设数量的历史实体对象；候选特异集合所包含的实体的数量为第二预设数量，第二预设数量可以根据实际需求所设定。

示例性的，对实体关联集合中存在的每一个历史实体对象所对应的目标关联度进行排序，取目标关联度排序中排名由高到低的第二预设数量个目标关联度，提取与第二预设数量个目标关联度所对应的各历史实体对象，并基于各历史实体对象构建候选特异集合。

示例性的，历史实体对象 1 的目标关联度为 0.7、历史实体对象 2 的目标关联度为 0.9、历史实体对象 3 的目标关联度为 0.75、历史实体对象 4 的目标关联度为 0.6、历史实体对象 5 的目标关联度为 0.8，按目标关联度由高到低排序，此时可以确定历史实体对象 2 的目标关联度最高，历史实体对象 4 的目标关联度最低。第二预设数量取 4，此时历史实体对象 1、历史实体对象 2、历史实体对象 3 与历史实体对象 5 构建候选特异集合。

（4）基于最大团算法对所述候选特异集合所包含的历史实体对象进行群组挖掘，得到至少一个特异群组。

在本实施例中，最大团算法是一种构建最大独立集合的算法。在本实施例中，最大独立集合可以理解为特异群组。特异群组可以理解为特定数量个历史实体对象的集合。

示例性的，将候选特异集合内的多个历史实体对象按最大团算法分成不同的类，每一类可以确定为一个特异群组。

示例性的，候选特异集合中存在历史实体对象 1、历史实体对象 2、历史实体对象 3 与历史实体对象 5 的四个历史实体对象。将上述四个历史实体对象按最大团算法进行群组挖掘，得到最终的特异群组数量。例如，群组挖掘确定（1，5）与（2，3）两个特异群组。

S204、计算每个特异群组的潜在威胁评分。

在本实施例中，潜在威胁评分可以理解为每一个特异群组中的历史实体对象之间的关联度评分。

示例性的，基于各个特异群组之间的各个历史实体对象的目标关联度之间的评分，确定特异群组的潜在威胁评分。

可选的，将所述特异群组所包含的每个所述历史实体对象的目标关联度的平均值确定为所述特异群组的潜在威胁评分。

示例性的，特异群组 A 中存在历史实体对象 1 与历史实体对象 5，此时历史实体对象 1 的目标关联度为 0.7，历史实体对象 5 的目标关联度为 0.6，可以基于两个历史实体对象之间目标关联度的平均值确定当前特异群组 A 的潜在威胁评分为 0.65。特异群组 B 中存在历史实体对象 2 与历史实体对象 3，此时历史实体对象 2 的目标关联度为 0.9，历史实体对象 3 的目标关联度为 0.75，可以基于两个历史实体对象之间目标关联度的平均值确定当前特异群组 B 的潜在威胁评分为 0.825。

S205、根据当前周期内获取到的当前实体对象的当前实体日志与每个特异群组所包含的历史实体对象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。

在本实施例中，当前实体对象在各特异群组中的威胁评分可以理解为当前获取到的实体对象与历史实体对象之间的关联度评分。

示例性的，提取当前日志中各当前实体对象的信息，确定当前实体对象与历史实体对象之间的关联度，确定为第一关联度，基于与各个历史实体对象之间第一关联度可以确定当前实体对象在各特异群组中的威胁评分。

根据当前周期内获取到的当前实体对象的当前实体日志与每个特异群组所

包含的历史实体对象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可以理解为：

（1）对当前周期内获取到的当前实体对象对应的当前实体日志进行特征提取，得到所述当前实体对象的第二特征矩阵。其中，所述历史实体日志和所述当前实体日志采用相同的特征提取方式。

在本实施例中，第二特征矩阵可以理解为当前实体对象的多维特征向量所构成的矩阵。

示例性的，对当前周期内获取到的当前实体对象对应的当前实体日志进行特征提取，得到当前实体对象的特征所构成的第二特征矩阵。其中，对当前实体日志的特征提取方式和对历史实体日志相同的特征提取方式相同。

（2）根据所述当前实体对象的第二特征矩阵和每个所述特异群组中的历史实体对象的第一特征矩阵，确定所述当前实体对象与所述特异群组中对应的历史实体对象之间的第一关联度。

在本实施例中，计算当前实体对象的第一特征矩阵与每个特异群组中历史实体对象的第二特征矩阵之间的关联度，根据该关联度分别确定为当前实体对象与对应的特异群组中的每个历史实体对象之间的第一关联度。

（3）将所述当前实体对象对应的第一关联度的最大值，确定为所述当前实体对象在各所述特异群组中的威胁评分。

在本实施例中，将当前实体对象与每个特异群组内历史实体对象所对应的第一关联度按关联度从高到低的顺序排序，取当前实体对象与每个特异群组内历史实体对象对应第一关联度的的最大值；将每个特异群组所对应的第一关联度最大值确定为当前实体对象与该特异群组的威胁评分。

示例性的，当前实体对象与特异群组 A 存在的历史实体对象 1 以及历史实体对象 5 的第一关联度分别为 0.6 与 0.8，可以确定当前实体对象与特异群组 A 对应的威胁评分为 0.8；当前实体对象与特异群组 B 存在的历史实体对象 2 以及历史实体对象 3 的第一关联度分别为 0.5 与 0.2，可以确定当前实体对象与特异群组 B 对应的威胁评分为 0.5。

S206、根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果。

在本实施例中，当前实体对象与各特异群组所对应的威胁评分存在不同的评分值，确定当前实体对象对应的威胁评分的最大值是否小于所有特异群组的潜在威胁评分，若小于，可以确定当前实体对象不存在威胁，若不小于，确定当前实体对象存在威胁。

示例性的，当前实体对象与特异群组 A 对应的威胁评分为 0.8，与特异群组 B 对应的威胁评分为 0.5，可以确定当前实体对象对应的威胁评分的最大值为 0.8。特异群组 A 的潜在威胁评分为 0.65，特异群组 B 的潜在威胁评分为 0.825。当前实体对象对应的威胁评分的最大值大于特异群组 A 的潜在威胁评分，小于特异群组 B 的潜在威胁评分，可以看出当前实体对象对应的威胁评分的最大值不满足小于全部特异群组的潜在威胁评分条件，确定当前实体对象存在威胁。

在本实施例中，通过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，得到各历史实体对象的第一特征矩阵；对于每个包含两个历史实体对象的历史实体对象组，根据历史实体对象组的第一特征矩阵之间的关联度确定历史实体对象组的第二关联度；根据各历史实体对象组的第二关联度确定至少一个特异群组；计算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对象的当前实体日志与每个特异群组所包含的历史实体对象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；根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果。通过采用上述技术方案，确定各个历史实体对象的关联度，并根据潜在威胁实体集合的个数以及差异性确定风险的评分高低，既可以确定已有的历史实体对象数据中包含的威胁评分，也可以计算新的当前实体对象数据的威胁评分。采用无监督的分析方法，基于威胁实体群组的方式确定威胁评分，减少了标注的成本，同时应对未知的威胁时有较高的灵活度。上述技术方案，有效降低了威胁评分的成本，加强了威胁评分检测的准确性，可以适应多种应用场景下的威胁检测。

作为实施例的第一可选实施例，在上述实施例基础上，本第一可选实施例还可以根据当前实体对象对应的威胁评分的最大值和各特异群组的潜在威胁评分，确定当前实体对象的威胁检测结果，包括：

判断当前实体对象对应的威胁评分的最大值是否小于所有特异群组的潜在威胁评分；若是，则确定当前实体对象不存在威胁；

若否，则确定当前实体对象存在威胁。

示例性的，确定当前实体对象的对应的威胁评分的最大值威胁评分与所有特异群组的潜在威胁评分，若当前实体对象对应的威胁评分的最大值的最大威胁评分小于所有特异群组的潜在威胁评分，可以确定当前实体对象不存在威胁；若当前实体对象对应的威胁评分的最大值的最大威胁评分大于或等于任一特异群组的潜在威胁评分，可以确定当前实体对象存在威胁。

示例性的，当前实体对象对应的威胁评分的最大值的最大威胁评分为 0.7，特异群组的潜在威胁评分包括 0.8、0.85、0.79，此时当前实体对象对应的威胁

评分的最大值的最大威胁评分小于所有特异群组的潜在威胁评分，则可以确定当前实体对象不存在威胁。

示例性的，当前实体对象的最大威胁评分对应的威胁评分的最大值为 0.7，特异群组的潜在威胁评分包括 0.63、0.7、0.72，此时当前实体对象的最大威胁评分对应的威胁评分的最大值大于潜在威胁评分 0.63 且等于另一潜在威胁评分 0.7，此时可以确定当前实体对象存在威胁。

图 3 是本申请实施例二所提供一种实体对象的威胁检测方法的架构示意图，如图 3 所示，首先采集历史数据，确定历史实体对象以及历史实体日志，并对采集到的历史实体对象的数据进行特征聚合计算，获得特征矩阵，基于特征矩阵之间的关联度确定特异群组，进行潜在威胁的挖掘，并确定潜在威胁评分。

同时可以采集当前实体对象的当前实体日志作为新的实体数据，并对采集到的当前实体对象的数据进行特征聚合计算，获得特征矩阵，基于当前实体对象特征矩阵与历史实体对象之间的特征矩阵关联度，与特异群组对应的潜在威胁评分进行比较，从而确定当前实体对象的威胁评分。

可以理解的是，当前实体对象的数据采集信息也可以随着时间推进作为历史实体对象的数据采集信息，继续参与进实体对象的威胁检测过程中。

实施例三

图 4 是本申请实施例三提供的一种实体对象的威胁检测装置的结构示意图。如图 4 所示，该装置包括：

历史威胁评分模块 31，设置为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，确定特异群组以及每个所述特异群组的潜在威胁评分；

当前威胁评分模块 32，设置为根据当前周期内获取到的当前实体对象的当前实体日志与每个所述特异群组所包含的历史实体对象的历史实体日志之间的第一关联度，确定所述当前实体对象在各所述特异群组中的威胁评分；

检测结果确定模块 33，设置为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。

通过采用上述技术方案，采集历史实体对象横向维度以及时间维度的实体日志，聚合具体实体多个阶段、多个场景的习惯对实体进行特征构建，使实体画像更加具体；根据攻击的少数相似性，构建特异群组并进行分析的方法，更

贴近实际攻击的特征。上述技术方案，有效降低了威胁检测成本，提高了对威胁评分判断的准确性，保证了实体对象威胁可参考的全面性。

可选的，历史威胁评分模块31，包括：

特征提取单元，设置为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，得到各所述历史实体对象的第一特征矩阵；

关联度确定单元，设置为对于每个包含两个历史实体对象的历史实体对象组，根据所述历史实体对象组的第一特征矩阵之间的关联度确定所述历史实体对象组的第二关联度；

实体群组确定单元，设置为根据各所述历史实体对象组的第二关联度确定至少一个特异群组；

威胁评分计算单元，设置为计算每个所述特异群组的潜在威胁评分。

可选的，特征提取单元，设置为通过以下方式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，得到各所述历史实体对象的第一特征矩阵：

获取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；

对于每个历史实体对象对应的历史实体日志的日志信息，基于会话标记进行会话切分得到至少一个完整会话；

对于各所述完整会话，提取所述完整会话在预设维度特征参数上的特征得到所述完整会话的特征向量；

对于各所述历史实体对象，根据所述历史实体对象对应的各所述完整会话的特征向量按照会话发生时间排列得到初始特征矩阵；

对各所述初始特征矩阵进行平均池化得到各所述历史实体对象的第一特征矩阵。

可选的，实体群组确定单元，设置为通过以下方式根据各所述历史实体对象组的第二关联度确定至少一个特异群组：

根据各所述历史实体对象组的第二关联度的排序，确定由第二关联度最大的第一预设数量的历史实体对象组构成的实体关联集合；

对所述实体关联集合所包含的每个所述历史实体对象，将所述历史实体对象所属的历史实体对象组的第二关联度的最大值确定为所述历史实体对象的目标关联度；

根据所述实体关联集合中各所述历史实体对象的目标关联度的排序，确定

由目标关联度最大的第二预设数量的历史实体对象构成的候选特异集合；

基于最大团算法对所述候选特异集合所包含的历史实体对象进行群组挖掘，得到特异群组。

在一实施例中，计算每个所述特异群组的潜在威胁评分包括：将所述特异群组所包含的每个所述历史实体对象的目标关联度的平均值确定为所述特异群组的潜在威胁评分。

可选的，当前威胁评分模块 32，设置为通过以下方式确定所述当前实体对象在各所述特异群组中的威胁评分：

对当前周期内获取到的当前实体对象对应的当前实体日志进行特征提取，得到所述当前实体对象的第二特征矩阵；其中，所述历史实体日志和所述当前实体日志采用相同的特征提取方式；

根据所述当前实体对象的第二特征矩阵和每个所述特异群组中的历史实体对象的第一特征矩阵，确定所述当前实体对象与所述特异群组中对应的历史实体对象之间的第一关联度；

将所述当前实体对象对应的第一关联度的最大值，确定为所述当前实体对象在各所述特异群组中的威胁评分。

可选的，检测结果确定模块 33，设置为通过以下方式确定所述当前实体对象的威胁检测结果：

判断所述当前实体对象对应的威胁评分的最大值是否小于所有特异群组的潜在威胁评分。若是，则确定所述当前实体对象不存在威胁；

若否，则确定所述当前实体对象存在威胁。

可选的，所述装置还包括特异群组确定模块，设置为若根据所述历史实体对象的历史实体日志确定不存在特异群组，则根据当前周期内获取到的当前实体对象的当前实体日志进行特征提取和关联度计算，确定是否存在特异群组；

若存在，则确定所述特异群组内的当前实体对象存在威胁；

若不存在，则确定所述当前实体对象不存在威胁。

本申请实施例所提供的实体对象的威胁检测装置可执行本申请任意实施例所提供的实体对象的威胁检测方法，具备执行方法相应的功能模块和有益效果。

实施例四

图 5 示出了可以用来实施本申请的实施例的电子设备 40 的结构示意图。电

子设备旨在表示各种形式的数字计算机，诸如，膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置，诸如，个人数字处理、蜂窝电话、智能电话、可穿戴设备（如头盔、眼镜、手表等）和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例。

如图 5 所示，电子设备 40 包括至少一个处理器 41，以及与至少一个处理器 41 通信连接的存储器，如只读存储器（Read Only Memory，ROM）42、随机访问存储器（Random Access Memory，RAM）43 等，其中，存储器存储有可被至少一个处理器执行的计算机程序，处理器 41 可以根据存储在只读存储器（ROM）42 中的计算机程序或者从存储单元 48 加载到随机访问存储器（RAM）43 中的计算机程序，来执行各种适当的动作和处理。在 RAM 43 中，还可存储电子设备 40 操作所需的各种程序和数据。处理器 41、ROM 42 以及 RAM 43 通过总线 44 彼此相连。输入/输出（Input/Output，I/O）接口 45 也连接至总线 44。

电子设备 40 中的多个部件连接至 I/O 接口 45，包括：输入单元 46，例如键盘、鼠标等；输出单元 47，例如各种类型的显示器、扬声器等；存储单元 48，例如磁盘、光盘等；以及通信单元 49，例如网卡、调制解调器、无线通信收发机等。通信单元 49 允许电子设备 40 通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

处理器 41 可以是各种具有处理和计算能力的通用和/或专用处理组件。处理器 41 的一些示例可以包括中央处理单元（Central Processing Unit，CPU）、图形处理单元（Graphic Processing Unit，GPU）、各种专用的人工智能（Artificial Intelligence，AI）计算芯片、各种运行机器学习模型算法的处理器、数字信号处理器（Digital Signal Processing，DSP）、以及任何适当的处理器、控制器、微控制器等。处理器 41 执行上文所描述的各个方法和处理，例如一种实体对象的威胁检测方法。

在一些实施例中，一种实体对象的威胁检测方法可被实现为计算机程序，其被有形地包含于计算机可读存储介质，例如存储单元 48。在一些实施例中，计算机程序的部分或者全部可以经由 ROM 42 和/或通信单元 49 而被载入和/或安装到电子设备 40 上。当计算机程序加载到 RAM 43 并由处理器 41 执行时，可以执行上文描述的实体对象的威胁检测方法的一个或多个步骤。备选地，在其他实施例中，处理器 41 可以通过其他适当的方式（例如，借助于固件）而被配置为执行一种实体对象的威胁检测方法。

本文中以上描述的系统和技术的各种实施方式可以在数字电子电路系统、集成电路系统、场可编程门阵列（Field-Programmable Gate Array，FPGA）、专

用集成电路（Application Specific Integrated Circuit，ASIC）、专用标准产品（Application Specific Standard Parts，ASSP）、芯片上系统的系统（System on Chip，SOC）、复杂可编程逻辑设备（Complex Programmable Logic Device，CPLD）、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括：实施在一个或者多个计算机程序中，该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，该可编程处理器可以是专用或者通用可编程处理器，可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令，并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

用于实施本申请的方法的计算机程序可以采用一个或多个编程语言的任何组合来编写。这些计算机程序可以提供给通用计算机、专用计算机或其他可编程数据处理装置的处理器，使得计算机程序当由处理器执行时使流程图和/或框图中所规定的功能/操作被实施。计算机程序可以完全在机器上执行、部分地在机器上执行，作为独立软件包部分地在机器上执行且部分地在远程机器上执行或完全在远程机器或服务器上执行。

在本申请的上下文中，计算机可读存储介质可以是有形的介质，其可以包含或存储以供指令执行系统、装置或设备使用或与指令执行系统、装置或设备结合地使用的计算机程序。计算机可读存储介质可以包括电子的、磁性的、光学的、电磁的、红外的、或半导体系统、装置或设备，或者上述内容的任何合适组合。备选地，计算机可读存储介质可以是机器可读信号介质。机器可读存储介质的示例可以包括基于一个或多个线的电气连接、便携式计算机盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦除可编程只读存储器（Electronic Programable Read Only Memory，EPROM）或快闪存储器、光纤、便捷式紧凑盘只读存储器（Compact Disc-Read Only Memory，CD-ROM）、光学储存设备、磁储存设备、或上述内容的合适组合。

为了提供与用户的交互，可以在电子设备上实施此处描述的系统和技术，该电子设备具有：用于向用户显示信息的显示装置（例如，阴极射线管（Cathode Ray Tube，CRT）或者液晶显示器（Liquid Crystal Display，LCD）或者监视器）；以及键盘和指向装置（例如，鼠标或者轨迹球），用户可以通过该键盘和该指向装置来将输入提供给电子设备。其它种类的装置还可以用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的传感反馈（例如，视觉反馈、听觉反馈、或者触觉反馈）；并且可以用任何形式（包括声输入、语音输入或者、触觉输入）来接收来自用户的输入。

可以将此处描述的系统和技术实施在包括后台部件的计算系统（例如，作

为数据服务器）、或者包括中间件部件的计算系统（例如，应用服务器）、或者包括前端部件的计算系统（例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互）、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信（例如，通信网络）来将系统的部件相互连接。通信网络的示例包括：局域网（Local Area Network，LAN）、广域网（Wide Area Network，WAN）、区块链网络和互联网。

计算系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。服务器可以是云服务器，又称为云计算服务器或云主机，是云计算服务体系中的一项主机产品，以解决了传统物理主机与VPS服务中，存在的管理难度大，业务扩展性弱的缺陷。

应该理解，可以使用上面所示的各种形式的流程，重新排序、增加或删除步骤。例如，本申请中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本申请的技术方案所期望的结果。

权 利 要 求 书

1. 一种实体对象的威胁检测方法，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所述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对象的当前实体日志与每个所述特异群组所包含的历史实体对象的历史实体日志之间的第一关联度，确定所述当前实体对象在各所述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。

2. 根据权利要求 1 所述的方法，其中，所述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所述特异群组的潜在威胁评分，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，得到各所述历史实体对象的第一特征矩阵；

对于每个包含两个历史实体对象的历史实体对象组，根据所述历史实体对象组的第一特征矩阵之间的关联度确定所述历史实体对象组的第二关联度；

根据各所述历史实体对象组的第二关联度确定至少一个特异群组；

计算每个所述特异群组的潜在威胁评分。

3. 根据权利要求 2 所述的方法，其中，所述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，得到各所述历史实体对象的第一特征矩阵，包括：

获取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；

对于每个历史实体对象对应的历史实体日志的日志信息，基于会话标记进行会话切分得到至少一个完整会话；

对于各所述完整会话，提取所述完整会话在预设维度特征参数上的特征得到所述完整会话的特征向量；

对于各所述历史实体对象，根据所述历史实体对象对应的各所述完整会话的特征向量按照会话发生时间排列得到初始特征矩阵；

对各所述初始特征矩阵进行平均池化得到各所述历史实体对象的第一特征矩阵。

4. 根据权利要求 2 所述的方法，其中，所述根据各所述历史实体对象组的第二关联度确定至少一个特异群组，包括：

根据各所述历史实体对象组的第二关联度的排序，确定由第二关联度最大的第一预设数量的历史实体对象组构成的实体关联集合；

对所述实体关联集合所包含的每个所述历史实体对象，将所述历史实体对象所属的历史实体对象组的第二关联度的最大值确定为所述历史实体对象的目标关联度；

根据所述实体关联集合中各所述历史实体对象的目标关联度的排序，确定由目标关联度最大的第二预设数量的历史实体对象构成的候选特异集合；

基于最大团算法对所述候选特异集合所包含的历史实体对象进行群组挖掘，得到至少一个特异群组。

5. 根据权利要求 4 所述的方法，其中，所述计算每个所述特异群组的潜在威胁评分，包括：

将所述特异群组所包含的每个所述历史实体对象的目标关联度的平均值确定为所述特异群组的潜在威胁评分。

6. 根据权利要求 1 所述的方法，其中，所述根据当前周期内获取到的当前实体对象的当前实体日志与每个所述特异群组所包含的历史实体对象的历史实体日志之间的第一关联度，确定所述当前实体对象在各所述特异群组中的威胁评分，包括：

对当前周期内获取到的当前实体对象对应的当前实体日志进行特征提取，得到所述当前实体对象的第二特征矩阵；其中，所述历史实体日志和所述当前实体日志采用相同的特征提取方式；

根据所述当前实体对象的第二特征矩阵和每个所述特异群组中的历史实体对象的第一特征矩阵，确定所述当前实体对象与所述特异群组中对应的历史实体对象之间的第一关联度；

将所述当前实体对象对应的第一关联度的最大值，确定为所述当前实体对象在各所述特异群组中的威胁评分。

7. 根据权利要求 1 所述的方法，其中，所述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，包括：

判断所述当前实体对象对应的威胁评分的最大值是否小于所有特异群组的潜在威胁评分；

若是，则确定所述当前实体对象不存在威胁；

若否，则确定所述当前实体对象存在威胁。

8. 根据权利要求 1 所述的方法，所述方法还包括：

若根据所述历史实体对象的历史实体日志确定不存在特异群组，则根据当前周期内获取到的当前实体对象的当前实体日志进行特征提取和关联度计算，确定是否存在特异群组；

若存在，则确定所述特异群组内的当前实体对象存在威胁；

若不存在，则确定所述当前实体对象不存在威胁。

9. 一种实体对象的威胁检测装置，包括：

历史威胁评分模块，设置为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，确定特异群组以及每个所述特异群组的潜在威胁评分；

当前威胁评分模块，设置为根据当前周期内获取到的当前实体对象的当前实体日志与每个所述特异群组所包含的历史实体对象的历史实体日志之间的第一关联度，确定所述当前实体对象在各所述特异群组中的威胁评分；

检测结果确定模块，设置为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。

10. 一种电子设备，所述电子设备包括：

至少一个处理器；以及

与所述至少一个处理器通信连接的存储器；其中，

所述存储器存储有可被所述至少一个处理器执行的计算机程序，所述计算机程序被所述至少一个处理器执行，以使所述至少一个处理器能够执行权利要求 1-8 中任一项所述的实体对象的威胁检测方法。

11. 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机指令，所述计算机指令用于使处理器执行时实现权利要求 1-8 中任一项所述的实体对象的威胁检测方法。