(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114510725 A
(43)申请公布日 2022.05.17

(21)申请号 202210207318.1

(22)申请日 2022.03.04

(71)申请人 泰安佳永信计算机有限公司
地址 271000 山东省泰安市泰山区岱庙街道青年路48号

(72)发明人 覃振森 魏享

(51)Int.Cl.
G06F 21/57(2013.01)

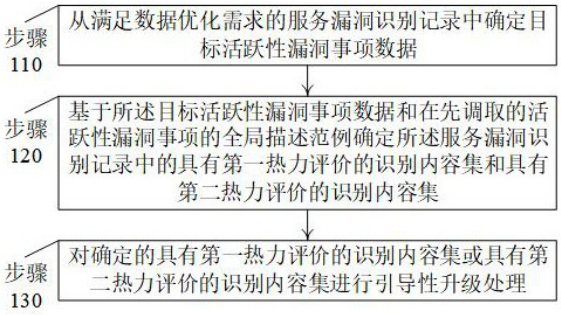
权利要求书3页 说明书14页 附图1页

(54)发明名称

一种基于数字化服务的漏洞信息处理方法及服务器

(57)摘要

本发明提供一种基于数字化服务的漏洞信息处理方法及服务器，可以利用从服务漏洞识别记录提取所得的目标活跃性漏洞事项数据来智能化且高效地确定需要进行引导性升级处理的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集，而不必耗费人力进行人工选取需进行引导性升级处理的识别内容集或者人工实施引导性升级处理，这样可以快速准确地实现对不同识别内容集的引导性升级处理，为后续的漏洞修复提供质量更高的判断依据。



CN 114510725 A

1.一种基于数字化服务的漏洞信息处理方法,其特征在于,应用于数字化服务器,所述方法至少包括:

利用已完成配置的服务漏洞分析模型,从满足数据优化需求的服务漏洞识别记录中提取目标活跃性漏洞事项,获取提取所得的目标活跃性漏洞事项数据;

基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集;对所述具有第一热力评价的识别内容集或所述具有第二热力评价的识别内容集进行引导性升级处理。

2.根据权利要求1所述的方法,其特征在于,所述服务漏洞分析模型根据第二认证知识序列中的部分已认证服务漏洞识别记录以及第三认证知识序列中的已认证服务漏洞识别记录联合配置所得;所述第二认证知识序列为根据待进行配置的服务漏洞分析模型对第一认证知识序列中没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的主题绑定所得,所述第三认证知识序列包括若干个完成主题绑定的已认证服务漏洞识别记录;

其中,所述服务漏洞分析模型用于提取丢失内容检测数据并通过如下思路在先配置所确定:确定第一认证知识序列,所述第一认证知识序列包括若干个没有进行主题绑定的已认证服务漏洞识别记录;基于服务漏洞分析模型,对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的分布主题绑定,得到第二认证知识序列,其中,所述服务漏洞分析模型用于对服务漏洞识别记录进行显著特征内容捕捉;至少基于所述第二认证知识序列中的部分已认证服务漏洞识别记录及第三认证知识序列,更新所述服务漏洞分析模型的模型变量,其中,所述第三认证知识序列包括若干个完成主题绑定的已认证服务漏洞识别记录;

其中,所述丢失内容检测数据包括:操作习惯显著特征内容、会话交互显著特征内容、文本显著特征内容、程序运行显著特征内容及身份验证显著特征内容中的其中一种或者几种的组合。

3.根据权利要求2所述的方法,其特征在于,所述基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集包括:

将所述活跃性漏洞事项的全局描述范例中至少部分识别内容集与提取所得的所述目标活跃性漏洞事项数据进行关联分析;

根据关联分析结果确定所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的比较内容;

基于所述比较内容更新所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述;

将完成更新的活跃性漏洞事项的全局描述迁移至所述服务漏洞识别记录中,获取所述服务漏洞识别记录中包括目标活跃性漏洞事项的具有第一热力评价的识别内容集以及涵盖至少部分非所述具有第一热力评价的识别内容集的具有第二热力评价的识别内容集;

其中,所述比较内容包括:所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的维度变化数据、误差统计数据和/或状态比对数据;

其中，所述服务漏洞识别记录为本地服务漏洞识别记录或远程服务漏洞识别记录；所述服务漏洞识别记录为远程服务漏洞识别记录，所述从满足数据优化需求的服务漏洞识别记录中提取目标活跃性漏洞事项，获取提取所得的目标活跃性漏洞事项数据：基于从在先的远程服务漏洞识别记录确定的目标活跃性漏洞事项数据从满足数据优化需求的远程服务漏洞识别记录确定所述目标活跃性漏洞事项数据；或者，利用对满足数据优化需求的远程服务日志进行依次的远程服务漏洞识别记录提取，确定各所述远程服务漏洞识别记录中的目标活跃性漏洞事项数据。

4.根据权利要求2或3中任一项所述的方法，其特征在于，所述方法还包括：

确定所述具有第一热力评价的识别内容集和具有第二热力评价的识别内容集之间的传递型内容集；

对所述传递型内容集进行引导性升级处理。

5.根据权利要求4所述的方法，其特征在于，所述对所述传递型内容集进行引导性升级处理包括：

对所述传递型内容集进行阶段化引导性升级处理或语义添加处理。

6.根据权利要求2或3中任一项所述的方法，其特征在于，所述从满足数据优化需求的服务漏洞识别记录中确定目标活跃性漏洞事项数据，包括：

获取活跃性漏洞事项命中标签；

基于所述活跃性漏洞事项命中标签从所述满足数据优化需求的服务漏洞识别记录中确定所述目标活跃性漏洞事项数据；

其中，所述目标活跃性漏洞事项数据包括如下最少一种：信息丢失事项数据、信息篡改事项数据、ddos事项数据、IP伪造事项数据、业务掉线事项数据、强制弹窗事项数据；

其中，所述信息丢失事项数据包括如下最少一种：丢失内容检测数据、丢失时段检测数据、丢失方式检测数据、丢失状态检测数据；

其中，所述活跃性漏洞事项的全局描述范例包括如下最少一种：具有信息丢失标签的全局描述范例、具有非法访问标签的全局描述范例、具有信息篡改标签的全局描述范例、具有ddos攻击标签的全局描述范例、具有指定风险标签的全局描述范例。

7.根据权利要求6所述的方法，其特征在于，所述在先调取的活跃性漏洞事项的全局描述范例包括：分别指向不同信息丢失状态的若干个具有非法访问标签的全局描述范例；

基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集之前，还包括：从所述在先调取的活跃性漏洞事项的全局描述范例当中确定与所述丢失状态检测数据对应的具有非法访问标签的全局描述范例。

8.根据权利要求2所述的方法，其特征在于，所述基于服务漏洞分析模型，对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到第二认证知识序列，包括：

对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理，得到第四认证知识序列，其中，所述服务漏洞识别记录转化处理包括：内容顺序调整、内容匿名处理、内容要素增减、扰动处理及内容替换处理中的其中一种或者几种的组合；

基于所述服务漏洞分析模型，对所述第四认证知识序列以及所述第一认证知识序列中的各已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到所述第二认证知识序列。

9.根据权利要求8所述的方法，其特征在于，所述至少基于所述第二认证知识序列中的部分已认证服务漏洞识别记录及第三认证知识序列，更新所述服务漏洞分析模型的模型变量，包括：

对于所述第一认证知识序列中的每个没有进行主题绑定的已认证服务漏洞识别记录，基于所述没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理后的显著特征内容分布数据，鉴别所述没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据是否为满足要求的认证示例；其中，所述没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据，及其进行服务漏洞识别记录转化处理后的显著特征内容分布数据皆涵盖于所述第二认证知识序列中；

基于所述第二认证知识序列中的各所述满足要求的认证示例及第三认证知识序列，更新所述服务漏洞分析模型的模型变量。

10.一种数字化服务器，其特征在于，包括：存储器和处理器；所述存储器和所述处理器耦合；所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令；其中，当所述处理器执行所述计算机指令时，使得所述数字化服务器执行如权利要求1-9中任意一项所述的方法。

一种基于数字化服务的漏洞信息处理方法及服务器

技术领域

[0001] 本发明涉及数字化服务技术领域，尤其涉及一种基于数字化服务的漏洞信息处理方法及服务器。

背景技术

[0002] 随着以互联网、大数据、人工智能为代表的新一代信息技术蓬勃发展，对社会经济、人民生活带来重大而深远的影响，也逐渐成为驱动企业经营管理和成长进步的新引擎，数字化服务转型也成为企业的核心战略。

[0003] 如今，在数字化基础上，各项服务可以极大的提高行业发展效率，然而服务进程下，服务漏洞难免会发生，相关技术为了避免上述问题的出现，大多选择人工方式进行漏洞分析处理，这样难以保障后期漏洞修复的质量。。

发明内容

[0004] 本发明提供一种基于数字化服务的漏洞信息处理方法及服务器，为实现上述技术目的，本发明采用如下技术方案。

[0005] 第一方面是一种基于数字化服务的漏洞信息处理方法，应用于数字化服务器，所述方法至少包括：

利用已完成配置的服务漏洞分析模型，从满足数据优化需求的服务漏洞识别记录中提取目标活跃性漏洞事项，获取提取所得的目标活跃性漏洞事项数据；

基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集；对所述具有第一热力评价的识别内容集或所述具有第二热力评价的识别内容集进行引导性升级处理。

[0006] 在一种可能的技术方案中，所述服务漏洞分析模型根据第二认证知识序列中的部分已认证服务漏洞识别记录以及第三认证知识序列中的已认证服务漏洞识别记录联合配置所得；所述第二认证知识序列为根据待进行配置的服务漏洞分析模型对第一认证知识序列中没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的主题绑定所得，所述第三认证知识序列包括若干个完成主题绑定的已认证服务漏洞识别记录；

其中，所述服务漏洞分析模型用于提取丢失内容检测数据并通过如下思路在先配置所确定：确定第一认证知识序列，所述第一认证知识序列包括若干个没有进行主题绑定的已认证服务漏洞识别记录；基于服务漏洞分析模型，对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到第二认证知识序列，其中，所述服务漏洞分析模型用于对服务漏洞识别记录进行显著特征内容捕捉；至少基于所述第二认证知识序列中的部分已认证服务漏洞识别记录及第三认证知识序列，更新所述服务漏洞分析模型的模型变量，其中，所述第三认证知识序列包括若干个完成主题绑定的已认证服务漏洞识别记录；

其中，所述丢失内容检测数据包括：操作习惯显著特征内容、会话交互显著特征内容、文本显著特征内容、程序运行显著特征内容及身份验证显著特征内容中的其中一种或者几种的组合。

[0007] 在一种可能的技术方案中，所述基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集包括：

将所述活跃性漏洞事项的全局描述范例中至少部分识别内容集与提取所得的所述目标活跃性漏洞事项数据进行关联分析；

根据关联分析结果确定所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的比较内容；

基于所述比较内容更新所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述；

将完成更新的活跃性漏洞事项的全局描述迁移至所述服务漏洞识别记录中，获取所述服务漏洞识别记录中包括目标活跃性漏洞事项的具有第一热力评价的识别内容集以及涵盖至少部分非所述具有第一热力评价的识别内容集的具有第二热力评价的识别内容集；

其中，所述比较内容包括：所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的维度变化数据、误差统计数据和/或状态比对数据；

其中，所述服务漏洞识别记录为本地服务漏洞识别记录或远程服务漏洞识别记录；所述服务漏洞识别记录为远程服务漏洞识别记录，所述从满足数据优化需求的服务漏洞识别记录中提取目标活跃性漏洞事项，获取提取所得的目标活跃性漏洞事项数据：基于从在先的远程服务漏洞识别记录确定的目标活跃性漏洞事项数据从满足数据优化需求的远程服务漏洞识别记录确定所述目标活跃性漏洞事项数据；或者，利用对满足数据优化需求的远程服务日志进行依次的远程服务漏洞识别记录提取，确定各所述远程服务漏洞识别记录中的目标活跃性漏洞事项数据。

[0008] 在一种可能的技术方案中，所述方法还包括：

确定所述具有第一热力评价的识别内容集和具有第二热力评价的识别内容集之间的传递型内容集；

对所述传递型内容集进行引导性升级处理。

[0009] 在一种可能的技术方案中，所述对所述传递型内容集进行引导性升级处理包括：

对所述传递型内容集进行阶段化引导性升级处理或语义添加处理。

[0010] 在一种可能的技术方案中，所述从满足数据优化需求的服务漏洞识别记录中确定目标活跃性漏洞事项数据，包括：

获取活跃性漏洞事项命中标签；

基于所述活跃性漏洞事项命中标签从所述满足数据优化需求的服务漏洞识别记录中确定所述目标活跃性漏洞事项数据；

其中，所述目标活跃性漏洞事项数据包括如下最少一种：信息丢失事项数据、信息

篡改事项数据、ddos事项数据、IP伪造事项数据、业务掉线事项数据、强制弹窗事项数据；

其中，所述信息丢失事项数据包括如下最少一种：丢失内容检测数据、丢失时段检测数据、丢失方式检测数据、丢失状态检测数据；

其中，所述活跃性漏洞事项的全局描述范例包括如下最少一种：具有信息丢失标签的全局描述范例、具有非法访问标签的全局描述范例、具有信息篡改标签的全局描述范例、具有ddos攻击标签的全局描述范例、具有指定风险标签的全局描述范例。

[0011] 在一种可能的技术方案中，所述在先调取的活跃性漏洞事项的全局描述范例包括：分别指向不同信息丢失状态的若干个具有非法访问标签的全局描述范例；

基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集之前，还包括：从所述在先调取的活跃性漏洞事项的全局描述范例当中确定与所述丢失状态检测数据对应的具有非法访问标签的全局描述范例。

[0012] 在一种可能的技术方案中，所述基于服务漏洞分析模型，对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到第二认证知识序列，包括：

对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理，得到第四认证知识序列，其中，所述服务漏洞识别记录转化处理包括：内容顺序调整、内容匿名处理、内容要素增减、扰动处理及内容替换处理中的其中一种或者几种的组合；

基于所述服务漏洞分析模型，对所述第四认证知识序列以及所述第一认证知识序列中的各已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到所述第二认证知识序列。

[0013] 在一种可能的技术方案中，所述至少基于所述第二认证知识序列中的部分已认证服务漏洞识别记录及第三认证知识序列，更新所述服务漏洞分析模型的模型变量，包括：

对于所述第一认证知识序列中的每个没有进行主题绑定的已认证服务漏洞识别记录，基于所述没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理后的显著特征内容分布数据，鉴别所述没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据是否为满足要求的认证示例；其中，所述没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据，及其进行服务漏洞识别记录转化处理后的显著特征内容分布数据皆涵盖于所述第二认证知识序列中；

基于所述第二认证知识序列中的各所述满足要求的认证示例及第三认证知识序列，更新所述服务漏洞分析模型的模型变量。

[0014] 第二方面是一种数字化服务器，包括存储器和处理器；所述存储器和所述处理器耦合；所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令；其中，当所述处理器执行所述计算机指令时，使得所述数字化服务器执行第一方面的方法。

[0015] 根据本发明的一个实施例，对满足数据优化需求的服务漏洞识别记录进行提取，以确定目标活跃性漏洞事项数据，根据确定的目标活跃性漏洞事项数据和活跃性漏洞事项的全局描述范例获取所述满足数据优化需求的服务漏洞识别记录中的具有第一热力评价的识别内容集以及具有第二热力评价的识别内容集，再对所述具有第二热力评价的识别内

容集或者具有第一热力评价的识别内容集进行引导性升级处理，这样可以利用从服务漏洞识别记录提取所得的目标活跃性漏洞事项数据来智能化且高效地确定需要进行引导性升级处理的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集，而不必耗费人力进行人工选取需进行引导性升级处理的识别内容集或者人工实施引导性升级处理，这样可以快速准确地实现对不同识别内容集的引导性升级处理，为后续的漏洞修复提供质量更高的判断依据。

附图说明

[0016] 图1为本发明实施例提供的一种基于数字化服务的漏洞信息处理方法的流程示意图。

[0017] 图2为本发明实施例提供的一种基于数字化服务的漏洞信息处理装置的模块框图。

具体实施方式

[0018] 以下，术语“第一”、“第二”和“第三”等仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”或“第三”等的特征可以明示或者隐含地包括一个或者更多个该特征。

[0019] 图1示出了本发明实施例提供的基于数字化服务的漏洞信息处理方法的流程示意图，基于数字化服务的漏洞信息处理方法可以通过数字化服务器实现，数字化服务器可以包括存储器和处理器；所述存储器和所述处理器耦合；所述存储器用于存储计算机程序代码，所述计算机程序代码包括计算机指令；其中，当所述处理器执行所述计算机指令时，使得所述数字化服务器执行如下步骤所描述的技术方案。

[0020] 步骤110，从满足数据优化需求的服务漏洞识别记录中确定目标活跃性漏洞事项数据。

[0021] 在本发明实施例中，满足数据优化需求的服务漏洞识别记录具备相应的特征识别度，进一步的，可以是通过采集线程（例如：合法网络爬虫等）检测到的服务漏洞识别记录，也可以是事先存储的服务漏洞识别记录（例如：历史服务事项中的服务漏洞识别记录），也可以是目标服务项目列表中的服务漏洞识别记录。该服务漏洞识别记录可以是以数字支付服务、数字办公服务、数字游戏服务为被检测的活跃性漏洞事项的服务漏洞识别记录，但不限于此。

[0022] 进一步地，数据优化需求的服务漏洞识别记录可以理解为待处理的服务漏洞识别记录，服务漏洞识别记录可以通过图文形式进行表示，但不限于此。

[0023] 在本发明实施例中，可以利用任意匹配的服务漏洞识别记录处理线程从该满足数据优化需求的服务漏洞识别记录确定/提取目标活跃性漏洞事项数据。提取所得的目标活跃性漏洞事项数据用于标记目标活跃性漏洞事项在服务漏洞识别记录中所对应的记录内容集。

[0024] 可以理解，目标活跃性漏洞事项数据可以是例如目标活跃性漏洞事项的状态、维度、核心的信息（例如：会话交互的状态、项目状态和维度等）、目标活跃性漏洞事项的显著特征内容（比如关键环节）、目标活跃性漏洞事项的标签信息等，但不限于此。

[0025] 步骤120,基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集。

[0026] 根据上述所描述的内容,步骤110确定的目标活跃性漏洞事项数据用于标记目标活跃性漏洞事项在服务漏洞识别记录中所对应的记录内容集,这样能够结合确定的目标活跃性漏洞事项数据以及反映目标活跃性漏洞事项的语义特征和信息量的活跃性漏洞事项的全局描述范例来分辨出目标活跃性漏洞事项在该满足数据优化需求的服务漏洞识别记录中所对应的记录内容集,并且将该目标活跃性漏洞事项在该满足数据优化需求的服务漏洞识别记录中所对应的记录内容集确定为服务漏洞识别记录的具有第一热力评价的识别内容集,而将该具有第一热力评价的识别内容集之外的至少局部服务漏洞识别记录集合确定为具有第二热力评价的识别内容集。

[0027] 进一步地,具有第一热力评价的识别内容集可以理解为较为活跃的识别内容集,具有第二热力评价的识别内容集可以理解为不活跃的识别内容集,对于本发明实施例而言,第一热力评价对应的评分值高于第二热力评价对应的评分值。在一些示例中,可以通过二分类的方法确定出具有第一热力评价的识别内容集以及具有第二热力评价的识别内容集,比如设置一个分类值,然后通过不同的热力评价对应的评分值对识别内容集进行二分类处理,这样能够实现对活跃程度不同的识别内容集的有效区分。

[0028] 步骤130,对确定的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集进行引导性升级处理。

[0029] 在本发明实施例中,能够结合具体服务环境的服务条件对具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集进行引导性升级处理。例如,可对确定的具有第二热力评价的识别内容集进行引导性升级处理,以在服务漏洞识别记录列表中标记出被检测到的目标活跃性漏洞事项,优化后续的漏洞修复思路。

[0030] 进一步地,引导性升级处理还可以理解为对具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集进行超链接处理或者索引配置处理,这样在后续进行漏洞修复时,通过具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集能够获取尽可能多的关联数据,从而为漏洞修复提供尽可能全面丰富的分析依据。

[0031] 可以理解,能够通过任意匹配的服务漏洞识别记录升级思路对具有第一热力评价的识别内容集或具有第二热力评价的识别内容集进行引导性升级处理。例如,通过设定引导性升级策略对具有第二热力评价的识别内容集或具有第一热力评价的识别内容集进行升级操作,本发明实施例还可以通过其它升级策略进行该引导性升级处理。

[0032] 由此可见,引导性升级处理能够丰富具有不同热力评价的识别内容集的特征信息,比如增设可视化的引导功能,以便于后续快速进行漏洞故障定位和溯源等。可以理解的是,引导性升级处理还可以理解为数据信息丰富处理,但不限于此。

[0033] 根据本发明实施例的基于数字化服务的漏洞信息处理方法,对满足数据优化需求的服务漏洞识别记录进行提取,以确定目标活跃性漏洞事项数据,根据确定的目标活跃性漏洞事项数据和活跃性漏洞事项的全局描述范例获取所述满足数据优化需求的服务漏洞识别记录中的具有第一热力评价的识别内容集以及具有第二热力评价的识别内容集,再对所述具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集进行引导性升

级处理，这样可以利用从服务漏洞识别记录提取所得的目标活跃性漏洞事项数据来智能化且高效地确定需要进行引导性升级处理的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集，而不必耗费人力进行人工选取需进行引导性升级处理的识别内容集或者人工实施引导性升级处理，这样可以快速准确地实现对不同识别内容集的引导性升级处理，为后续的漏洞修复提供质量更高的判断依据。

[0034] 对于另一些可独立实施的设计思路而言，基于数字化服务的漏洞信息处理方法还可以通过以下方式实现。

[0035] 步骤210，从满足数据优化需求的服务漏洞识别记录中确定目标活跃性漏洞事项数据。

[0036] 基于以上所描述的内容，可以利用任何匹配的服务漏洞识别记录处理线程从该满足数据优化需求的服务漏洞识别记录提取与目标活跃性漏洞事项数据，并且提取所得的目标活跃性漏洞事项数据用于标记目标活跃性漏洞事项在服务漏洞识别记录中所对应的记录内容集。

[0037] 可以理解，目标活跃性漏洞事项可以是数字支付服务、数字办公服务等(如信息篡改事项、业务掉线事项)。确定的目标活跃性漏洞事项数据可以包括如下最少一种：信息丢失事项数据、信息篡改事项数据、ddos事项数据、IP伪造事项数据、业务掉线事项数据、强制弹窗事项数据，本发明实施例提供的漏洞事项不限于以上信息。这些目标活跃性漏洞事项数据皆表征在检测有该活跃性漏洞事项的服务漏洞识别记录中活跃性漏洞事项的局部描述内容。

[0038] 在一种可能的实施例中，步骤210示例性的可以包括步骤212和步骤213。

[0039] 步骤212，获取活跃性漏洞事项命中标签。可以理解，该活跃性漏洞事项命中标签可以理解为服务漏洞识别记录集合的信息、活跃性漏洞事项的类别信息、活跃性漏洞事项标签信息等。

[0040] 步骤213，基于所述活跃性漏洞事项命中标签从所述满足数据优化需求的服务漏洞识别记录中确定所述目标活跃性漏洞事项数据。

[0041] 举例而言，依据指定的服务漏洞识别记录集合的信息，在指定的服务漏洞识别记录集合确定目标活跃性漏洞事项数据。

[0042] 步骤212和步骤213所描述的内容，可根据另外提供的活跃性漏洞事项命中标签(比如选择信息)来对服务漏洞识别记录进行提取，获取目标活跃性漏洞事项数据。

[0043] 在实际实施时，在另一种可能的实施例中，步骤210示例性的还可以包括：步骤214，从满足数据优化需求的服务漏洞识别记录中提取目标活跃性漏洞事项，获取提取所得的目标活跃性漏洞事项数据。换言之，首先从服务漏洞识别记录中提取得到目标活跃性漏洞事项，其次依据提取所得的目标活跃性漏洞事项确定目标活跃性漏洞事项数据。

[0044] 可以理解，能够利用已完成配置的服务漏洞分析模型从所述满足数据优化需求的服务漏洞识别记录中提取目标活跃性漏洞事项，以获取提取所得的目标活跃性漏洞事项数据。在实际实施时，可利用注释有用户活跃性漏洞事项数据的已认证服务漏洞识别记录事先调试用于提取用户活跃性漏洞事项的服务漏洞分析模型，用于提取例如数字游戏服务、信息丢失事项、数字办公服务等的服务漏洞分析模型。在提取处理中，将满足数据优化需求的服务漏洞识别记录加载至该服务漏洞分析模型，利用服务漏洞分析模型的提取处理来获

取目标活跃性漏洞事项数据。

[0045] 可以理解，该满足数据优化需求的服务漏洞识别记录可以是检测到的本地服务漏洞识别记录，也可以是识别到的远程服务集合中的远程服务漏洞识别记录，也可以是云服务日志中的远程服务漏洞识别记录。

[0046] 可以理解，在另一种可能的实施例中，步骤210示例性的还可以包括：步骤215，基于从在先的远程服务漏洞识别记录确定的目标活跃性漏洞事项数据从满足数据优化需求的远程服务漏洞识别记录确定所述目标活跃性漏洞事项数据。相同目标活跃性漏洞事项在持续的远程服务漏洞之间所对应的状态和维度趋于类似，这样可以依据从前一或前几个远程服务漏洞识别记录确定的目标活跃性漏洞事项数据从当前待提取的远程服务漏洞识别记录来提取满足数据优化需求的远程服务漏洞识别记录的目标活跃性漏洞事项数据，从而提高提取质量。

[0047] 或者，在另一种可能的实施例中，步骤210示例性的还可以包括：步骤216，利用对满足数据优化需求的远程服务日志进行依次的远程服务漏洞识别记录提取，确定各所述远程服务漏洞识别记录中的目标活跃性漏洞事项数据。利用对远程服务日志中的远程服务漏洞识别记录进行顺序提取，利用各远程服务漏洞识别记录的提取结果分别进行各远程服务漏洞识别记录的不同热力评价的识别内容集引导性升级处理，这样能够保障提取的精确性，由于每一远程服务漏洞识别记录都进行了引导性升级处理，继而从全局远程服务日志来看，可以实现目标活跃性漏洞事项的持续性引导性升级处理。

[0048] 可以理解的是，上述内容所记录的满足数据优化需求的远程服务日志中的远程服务漏洞可以代表远程服务日志中实际的漏洞，也可表示为远程服务日志中需要进行处理的识别记录，本发明实施例对此不作限制。

[0049] 根据以上其中一种可能的实施例的操作，从满足数据优化需求的服务漏洞识别记录中提取到目标活跃性漏洞事项数据。

[0050] 步骤220，基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集。

[0051] 在实际实施时，步骤220所记录的内容示例性的可以通过如下步骤221-步骤229所记录的技术方案实现。

[0052] 步骤221，将所述活跃性漏洞事项的全局描述范例中至少部分识别内容集与提取所得的所述目标活跃性漏洞事项数据进行关联分析(比如匹配处理)。

[0053] 可以理解，活跃性漏洞事项的全局描述范例可以涵盖如下最少一种：具有信息丢失标签的全局描述范例、具有非法访问标签的全局描述范例、具有信息篡改标签的全局描述范例、具有ddos攻击标签的全局描述范例、具有指定风险标签的全局描述范例等。具有信息丢失标签的全局描述范例用于关联分析信息丢失事项中的恶意行为，具有非法访问标签的全局描述范例用于关联分析非法访问事项中的访问行为，具有信息篡改标签的全局描述范例用于关联分析服务漏洞识别记录中数字游戏服务上的信息篡改事项描述，具有指定风险标签的全局描述范例用于关联分析具有指定攻击主题的事项的特征，如数据钓鱼等。

[0054] 在具体实施时，可以将活跃性漏洞事项的全局描述范例中至少部分识别内容集与提取所得的所述目标活跃性漏洞事项数据进行关联分析。举例而言，若确定的目标活跃性

漏洞事项数据是数字游戏服务的信息篡改事项数据，而数字游戏服务的信息篡改事项一般配置在数字游戏服务的核心环节，则可将数字游戏服务核心的互动环节相较于信息篡改事项的状态进行关联分析。另外，鉴于在进行检测时一般难以检测到活跃性漏洞事项的所有事件，因此在关联分析时可将活跃性漏洞事项的全局描述范例的部分识别内容集与确定的目标活跃性漏洞事项数据进行关联分析，以确定目标活跃性漏洞事项在服务漏洞识别记录中所对应的记录内容集。

[0055] 步骤223，根据关联分析结果确定所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的比较内容。

[0056] 在本发明实施例中，由于表征活跃性漏洞事项相似描述的活跃性漏洞事项的全局描述范例与满足数据优化需求的服务漏洞识别记录中的活跃性漏洞事项维度一般不会是相同维度，并且活跃性漏洞事项的状态、通道数等与活跃性漏洞事项的全局描述范例中的状态、通道数等一般会存在差异，因此在进行关联分析的过程中，需要首先将活跃性漏洞事项的全局描述范例进行内容要素增减、内容匿名处理和/或内容顺序调整，再与确定的活跃性漏洞事项的状态、维度或显著特征内容进行关联分析，从而获取活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述满足数据优化需求的服务漏洞识别记录中的活跃性漏洞事项的全局描述之间的比较内容(比如可以理解为差异信息)。

[0057] 可以理解，该比较内容可以包括活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的维度变化数据和/或误差统计数据等，还可包括活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述与所述服务漏洞识别记录中的目标活跃性漏洞事项的全局描述之间的状态比对数据等，但不限于上述所描述的内容。

[0058] 步骤225，基于所述比较内容更新所述活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述。

[0059] 在本发明实施例中，根据包括以上维度变化数据、误差统计数据等的比较内容将活跃性漏洞事项的全局描述范例中的活跃性漏洞事项的全局描述进行内容要素增减、内容匿名处理、内容顺序调整等，以与服务漏洞识别记录中目标活跃性漏洞事项所在的集合相关联分析。

[0060] 步骤227，将完成更新的活跃性漏洞事项的全局描述迁移至满足数据优化需求的服务漏洞识别记录中，获取所述服务漏洞识别记录中包括目标活跃性漏洞事项的具有第一热力评价的识别内容集以及涵盖至少部分非所述具有第一热力评价的识别内容集的具有第二热力评价的识别内容集。

[0061] 在本发明实施例中，利用将完成更新的活跃性漏洞事项的全局描述迁移至满足数据优化需求的服务漏洞识别记录中，可以将满足数据优化需求的服务漏洞识别记录中命中更新的约束区间内的识别内容确定为包括目标活跃性漏洞事项的具有第一热力评价的识别内容集，该具有第一热力评价的识别内容集内为目标活跃性漏洞事项所对应的记录内容集。另外，将包括具有第一热力评价的识别内容集之外的服务漏洞识别记录集合或者包括部分不具有第一热力评价的识别内容集的服务漏洞识别记录集合确定为该服务漏洞识别记录的具有第二热力评价的识别内容集。

[0062] 步骤229，确定所述具有第一热力评价的识别内容集和具有第二热力评价的识别内容集之间的传递型内容集。

[0063] 在本发明实施例中，可将具有第二热力评价的识别内容集中与目标活跃性漏洞事项所在集合的边界的量化比较指标小于在先调取的设定指标的服务漏洞识别记录集合确定为该传递型内容集。换言之，将目标活跃性漏洞事项的全局描述的边界进行调整，将调整的集合(识别内容集)作为该传递型内容集(中间型内容集)。

[0064] 在实施完步骤221-步骤229所记录的技术方案后，继续实施步骤230，对确定的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集进行引导性升级处理，并且对确定的传递型内容集进行阶段化引导性升级处理或语义添加处理。

[0065] 可以理解的是，对确定的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集进行的引导性升级处理与步骤130的实施方式类似，本发明在此不作过多描述。对传递型内容集可实施阶段化引导性升级处理或语义添加处理，以使引导性升级处理的效果更加准确。

[0066] 根据本发明实施例的基于数字化服务的漏洞信息处理方法，以多种方式对满足数据优化需求的本地服务漏洞识别记录或远程服务漏洞识别记录进行提取，确定本地服务漏洞识别记录或远程服务漏洞识别记录中的目标活跃性漏洞事项数据，根据确定的目标活跃性漏洞事项数据和活跃性漏洞事项的全局描述范例获取所述满足数据优化需求的服务漏洞识别记录中的具有第一热力评价的识别内容集、具有第二热力评价的识别内容集以及其间的传递型内容集，再对所述具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集进行引导性升级处理并对传递型内容集进行引导性升级处理，这样可以利用从本地服务漏洞识别记录或远程服务漏洞识别记录提取所得的目标活跃性漏洞事项数据来智能化且高效地确定需要进行引导性升级处理的具有第一热力评价的识别内容集、具有第二热力评价的识别内容集以及传递型内容集，而不必耗费人力进行人工选取需进行引导性升级处理的识别内容集或者人工实施引导性升级处理，这样可以快速准确地实现对不同识别内容集的引导性升级处理，为后续的漏洞修复提供质量更高的判断依据。

[0067] 在另一些可独立实施的设计思路下，基于数字化服务的漏洞信息处理方法的实现方式可以包括如下内容。示例性的，以丢失内容检测数据作为信息丢失事项数据。可以理解的是，以丢失内容检测数据作为信息丢失事项数据只是一种可能的实施例，本发明不限于此，信息丢失事项数据还可以包括丢失时段检测数据、丢失方式检测数据以及丢失状态检测数据当中的一个或若干个。

[0068] 步骤310，从满足数据优化需求的服务漏洞识别记录提取信息丢失事项数据。

[0069] 在本发明实施例中，利用已完成配置的显著特征内容捕捉网络从满足数据优化需求的服务漏洞识别记录提取丢失内容检测数据，将提取所得的丢失内容检测数据作为信息丢失事项数据。

[0070] 此外，对于步骤310而言，还可以从满足数据优化需求的服务漏洞识别记录提取丢失状态检测数据。

[0071] 步骤320，从所述在先调取的具有非法访问标签的全局描述范例当中确定与所述丢失状态检测数据对应的具有非法访问标签的全局描述范例。

[0072] 步骤330，基于所述信息丢失事项数据和在先调取的具有非法访问标签的全局描

述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集。步骤330的处理与以上步骤120或步骤221-步骤229的实施方式类似，本发明在此不作过多描述。

[0073] 步骤340，对所述具有第一热力评价的识别内容集或所述具有第二热力评价的识别内容集进行引导性升级处理。该步骤与步骤130的实施方式类似，本发明在此不作过多描述。

[0074] 根据本发明实施例三的基于数字化服务的漏洞信息处理方法，利用对满足数据优化需求的服务漏洞识别记录进行提取，获取信息丢失事项数据，根据提取所得的信息丢失事项数据和指定的全局描述范例获取所述满足数据优化需求的服务漏洞识别记录中的具有第一热力评价的识别内容集以及具有第二热力评价的识别内容集，再对所述具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集进行引导性升级处理，从而在对与指定漏洞事项相关的服务漏洞识别记录进行处理时，可利用从服务漏洞识别记录提取所得的信息丢失事项数据来智能化且高效地、准确地确定需要进行处理的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集，以对具有第一热力评价的识别内容集或具有第二热力评价的识别内容集执行引导性升级处理，而不必耗费人力进行人工选取需进行引导性升级处理的识别内容集，这样可以快速准确地实现对不同识别内容集的引导性升级处理，为后续的漏洞修复提供质量更高的判断依据。

[0075] 在另外的一种可独立实施的设计思路下，还包括对相关网络模型的训练方案。

[0076] 步骤510，确定第一认证知识序列，所述第一认证知识序列包括若干个没有进行主题绑定的已认证服务漏洞识别记录。

[0077] 在本发明实施例中，通常将加载至网络中的已完成注释有显著特征内容分布数据的服务漏洞识别记录，称为完成主题绑定的已认证服务漏洞识别记录。其中，显著特征内容分布数据是指显著特征内容在服务漏洞识别记录特征空间中的空间分布。在实际实施时，可以利用智能注释(标注)等方式预先对已认证服务漏洞识别记录进行显著特征内容的分布主题绑定。

[0078] 举例而言，以丢失内容检测数据为例，注释的丢失内容检测数据主要对应于在信息丢失事项运行中段和身份验证，丢失内容检测数据如操作习惯显著特征内容、会话交互显著特征内容、文本显著特征内容、身份验证显著特征内容等。丢失内容检测数据分布数据是丢失内容检测数据在信息丢失事项的服务漏洞识别记录特征空间中的空间分布。

[0079] 步骤520，基于服务漏洞分析模型，对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到第二认证知识序列，其中，所述服务漏洞分析模型用于对服务漏洞识别记录进行显著特征内容捕捉。

[0080] 可以理解的是，服务漏洞分析模型可以为AI模型(不限于CNN、GCN、RNN、LSTM)。由于服务漏洞分析模型可以是用于对服务漏洞识别记录进行显著特征内容捕捉的，因此，将第一认证知识序列中的各没有进行主题绑定的已认证服务漏洞识别记录加载至服务漏洞分析模型中，就可以对每一个没有进行主题绑定的已认证服务漏洞识别记录实现显著特征内容的分布主题绑定。可以理解的是，显著特征内容的分布主题绑定就是将没有进行主题绑定的已认证服务漏洞识别记录中的显著特征内容分布数据(比如空间分布)注释出来。

[0081] 可以理解，显著特征内容包括：丢失内容检测数据、主题显著特征内容、行为习惯

显著特征内容及业务场景显著特征内容中的其中一种或者几种的组合。当显著特征内容包括丢失内容检测数据时，丢失内容检测数据包括：操作习惯显著特征内容、会话交互显著特征内容、文本显著特征内容、程序运行显著特征内容及身份验证显著特征内容中的其中一种或者几种的组合。

[0082] 举例而言，以涵盖信息丢失事项的没有进行主题绑定的已认证服务漏洞识别记录为例，将涵盖信息丢失事项的没有进行主题绑定的已认证服务漏洞识别记录导入服务漏洞分析模型，导出是没有进行主题绑定的已认证服务漏洞识别记录自身，以及没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据，如操作习惯显著特征内容的空间分布、会话交互显著特征内容的空间分布等。

[0083] 鉴于此，当若干个包含信息丢失事项的没有进行主题绑定的已认证服务漏洞识别记录加载至服务漏洞分析模型时，许多的没有进行主题绑定的已认证服务漏洞识别记录自身，以及没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据形成了该步骤中的第二认证知识序列。

[0084] 步骤530，至少基于所述第二认证知识序列中的部分已认证服务漏洞识别记录及第三认证知识序列，更新所述服务漏洞分析模型的模型变量，其中，所述第三认证知识序列包括若干个完成主题绑定的已认证服务漏洞识别记录。

[0085] 举例而言，可以使用第二认证知识序列中的部分已认证服务漏洞识别记录或者全部已认证服务漏洞识别记录，以及第三认证知识序列一起更新服务漏洞分析模型的模型变量。这里，完成主题绑定的已认证服务漏洞识别记录可以参阅本实施例步骤510中的所描述的内容，本发明实施例不进行展开。

[0086] 利用本实施例提供的网络调试思路，利用两个认证知识序列更新服务漏洞分析模型的模型变量，其中一个是第二认证知识序列，该第二认证知识序列来源于基于服务漏洞分析模型，对包括若干个没有进行主题绑定的已认证服务漏洞识别记录的第一认证知识序列进行显著特征内容的分布主题绑定获取的。另一个是包括若干个完成主题绑定的已认证服务漏洞识别记录的第三认证知识序列。进一步地，认证知识序列可以理解为训练样本集。

[0087] 然而，与相关技术中需要对相关的AI模型的服务漏洞识别记录中的显著特征内容进行智能注释相比，本发明实施例可以实现在加载至模型的服务漏洞识别记录并不是非所有为已注释服务漏洞识别记录的情况下，提高显著特征内容捕捉网络的调试精度，换言之，这样不仅可以节省大量的资源，同时还可以显著提高网络调试的效率。

[0088] 在另外的一些设计思路下，步骤520可包括以下处理方式：对所述第一认证知识序列中的各所述没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理，得到第四认证知识序列，其中，所述服务漏洞识别记录转化处理包括：内容顺序调整、内容匿名处理、内容要素增减、扰动处理及内容替换处理中的其中一种或者几种的组合，但不限于此；基于所述服务漏洞分析模型，对所述第四认证知识序列以及所述第一认证知识序列中的各已认证服务漏洞识别记录进行显著特征内容的分布主题绑定，得到所述第二认证知识序列。

[0089] 由于第四认证知识序列和第一认证知识序列中均是没有进行主题绑定的已认证服务漏洞识别记录，那么基于与以上实施例一中说明的相同原理，将没有进行主题绑定的已认证服务漏洞识别记录导入服务漏洞分析模型，导出第四认证知识序列以及第一认证知

识序列中的各已认证服务漏洞识别记录的本身，以及各已认证服务漏洞识别记录的显著特征内容分布数据。

[0090] 另外，在其他的设计思路下，步骤330示例性可以包括：对于所述第一认证知识序列中的每个没有进行主题绑定的已认证服务漏洞识别记录，基于所述没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理后的显著特征内容分布数据，鉴别所述没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据是否为满足要求的认证示例；其中，所述没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据，及其进行服务漏洞识别记录转化处理后的显著特征内容分布数据皆涵盖于所述第二认证知识序列中；基于所述第二认证知识序列中的各所述满足要求的认证示例及第三认证知识序列，更新所述服务漏洞分析模型的模型变量。

[0091] 其中，没有进行主题绑定的已认证服务漏洞识别记录的显著特征内容分布数据，及其进行服务漏洞识别记录转化处理后的显著特征内容分布数据皆涵盖于第二认证知识序列中。

[0092] 将该没有进行主题绑定的已认证服务漏洞识别记录进行服务漏洞识别记录转化处理后的显著特征内容分布数据，进行服务漏洞识别记录优化操作(比如记录修正处理)。可以理解的是，服务漏洞识别记录优化操作可以理解为上述服务漏洞识别记录转化处理的逆向转化处理(比如反变换处理)。

[0093] 在一些可独立实施的设计思路下，在对所述具有第一热力评价的识别内容集或所述具有第二热力评价的识别内容集进行引导性升级处理之后，该方法还可以包括以下内容：如果完成引导性升级处理的为所述具有第一热力评价的识别内容集，则确定具有第一热力评价的识别内容集的漏洞修复引导特征；通过所述漏洞修复引导特征确定针对所述满足数据优化需求的服务漏洞识别记录的漏洞修复方针；基于设定指令激活所述漏洞修复方针。

[0094] 举例而言，可以根据完成引导性升级处理的具有第一热力评价的识别内容集对应的索引标签或者可视化引导主题尽可能全面地挖掘漏洞修复引导特征，该漏洞修复引导特征记录了漏洞修复的需求信息，从而可以基于漏洞修复引导特征完整准确确定出漏洞修复方针，然后根据设定指令在目标时段或者目标服务场景下激活该漏洞修复方针，这样可以实现针对性的漏洞修复。

[0095] 在一些可独立实施的设计思路下，通过所述漏洞修复引导特征确定针对所述满足数据优化需求的服务漏洞识别记录的漏洞修复方针，可以包括以下内容：提取所述漏洞修复引导特征中的阶段化修复需求描述分布和任务化修复需求描述分布；基于所述漏洞修复引导特征中的阶段化修复需求描述分布和任务化修复需求描述分布之间的描述分布相关度，对所述漏洞修复引导特征中的阶段化修复需求描述分布和任务化修复需求描述分布进行联合分析，得到描述分布联合分析结果；将联合分析存在异常的任务化修复需求描述分布确定为待关联任务化修复需求描述分布，根据所述描述分布联合分析结果中的任务化修复需求描述分布与所述待关联任务化修复需求描述分布之间的描述分布余弦差异，确定与所述待关联任务化修复需求描述分布相关联的服务偏好要素；对与所述待关联任务化修复需求描述分布相关联的服务偏好要素和所述待关联任务化修复需求描述分布进行联合分析，得到偏好要素联合分析结果；根据所述偏好要素联合分析结果和所述描述分布联合分

析结果，确定所述漏洞修复引导特征中的服务关注特征和所述服务关注特征对应的服务偏好要素，基于所述服务关注特征和所述服务关注特征对应的服务偏好要素生成漏洞修复方针。

[0096] 如此设计，通过考虑阶段化修复需求描述分布和任务化修复需求描述分布，能够尽可能完整地定位服务关注特征和服务关注特征对应的服务偏好要素，从而保障生成的漏洞修复方针的针对性和服务场景适配性。

[0097] 在一些可独立实施的设计思路下，所述提取漏洞修复引导特征中的阶段化修复需求描述分布和任务化修复需求描述分布，包括：提取所述漏洞修复引导特征中的至少两个阶段化修复需求信息和至少两个任务化修复需求信息；提取所述至少两个阶段化修复需求信息之间的阶段化修复需求信息余弦差异和阶段化修复需求信息差异，提取所述至少两个任务化修复需求信息之间的任务化修复需求信息余弦差异和任务化修复需求信息差异；根据所述阶段化修复需求信息余弦差异和所述阶段化修复需求信息差异，对所述至少两个阶段化修复需求信息进行拼接，得到所述漏洞修复引导特征中的阶段化修复需求描述分布；一个阶段化修复需求描述分布包括至少一个阶段化修复需求信息；根据所述任务化修复需求信息余弦差异和所述任务化修复需求信息差异，对所述至少两个任务化修复需求信息进行拼接，得到所述漏洞修复引导特征中的任务化修复需求描述分布；一个任务化修复需求描述分布包括至少一个任务化修复需求信息。如此设计，可以完整准确地获得阶段化修复需求描述分布和任务化修复需求描述分布。

[0098] 在一些可独立实施的设计思路下，所述基于所述漏洞修复引导特征中的阶段化修复需求描述分布和任务化修复需求描述分布之间的描述分布相关度，对所述漏洞修复引导特征中的阶段化修复需求描述分布和任务化修复需求描述分布进行联合分析，得到描述分布联合分析结果，包括：将所述漏洞修复引导特征中的任务化修复需求描述分布确定为衍生任务化修复需求描述分布，将所述漏洞修复引导特征中的阶段化修复需求描述分布确定为衍生阶段化修复需求描述分布；所述衍生任务化修复需求描述分布中的任务化修复需求信息是从针对所述漏洞修复引导特征的目标监测信息中所抽取的；提取所述目标监测信息中的阶段化修复需求信息；将所述目标监测信息中的阶段化修复需求信息与所述衍生阶段化修复需求描述分布中的阶段化修复需求信息之间的信息余弦差异，确定为所述衍生任务化修复需求描述分布与所述衍生阶段化修复需求描述分布之间的所述描述分布相关度；当所述描述分布相关度大于或等于相关度判定值时，对所述衍生任务化修复需求描述分布和所述衍生阶段化修复需求描述分布进行联合分析，得到所述描述分布联合分析结果。如此设计，可以避免描述分布联合分析结果存在缺失。

[0099] 基于同样的发明构思，图2示出了本发明实施例提供的基于数字化服务的漏洞信息处理装置的模块框图，一种基于数字化服务的漏洞信息处理装置可以包括实施图1所示的相关方法步骤的如下模块。

[0100] 数据获取模块21，用于从满足数据优化需求的服务漏洞识别记录中确定目标活跃性漏洞事项数据。

[0101] 内容集确定模块22，用于基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集。

[0102] 内容升级模块23,用于对确定的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集进行引导性升级处理。

[0103] 应用于本发明的相关实施例可以达到如下技术效果:对满足数据优化需求的服务漏洞识别记录进行提取,以确定目标活跃性漏洞事项数据,根据确定的目标活跃性漏洞事项数据和活跃性漏洞事项的全局描述范例获取所述满足数据优化需求的服务漏洞识别记录中的具有第一热力评价的识别内容集以及具有第二热力评价的识别内容集,再对所述具有第二热力评价的识别内容集或者具有第一热力评价的识别内容集进行引导性升级处理,这样可以利用从服务漏洞识别记录提取所得的目标活跃性漏洞事项数据来智能化且高效地确定需要进行引导性升级处理的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集,而不必耗费人力进行人工选取需进行引导性升级处理的识别内容集或者人工实施引导性升级处理,这样可以快速准确地实现对不同识别内容集的引导性升级处理,为后续的漏洞修复提供质量更高的判断依据。

[0104] 以上所述,仅为本发明的具体实施方式。熟悉本技术领域的技术人员根据本发明提供的具体实施方式,可想到变化或替换,都应涵盖在本发明的保护范围之内。

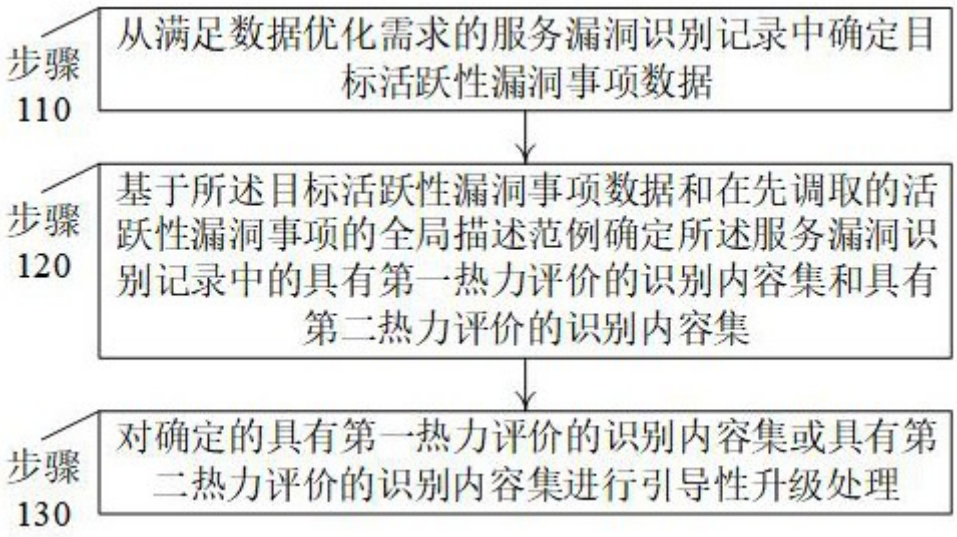

步骤
110
从满足数据优化需求的服务漏洞识别记录中确定目标活跃性漏洞事项数据
步骤
120
基于所述目标活跃性漏洞事项数据和在先调取的活跃性漏洞事项的全局描述范例确定所述服务漏洞识别记录中的具有第一热力评价的识别内容集和具有第二热力评价的识别内容集
步骤
130
对确定的具有第一热力评价的识别内容集或具有第二热力评价的识别内容集进行引导性升级处理

图1

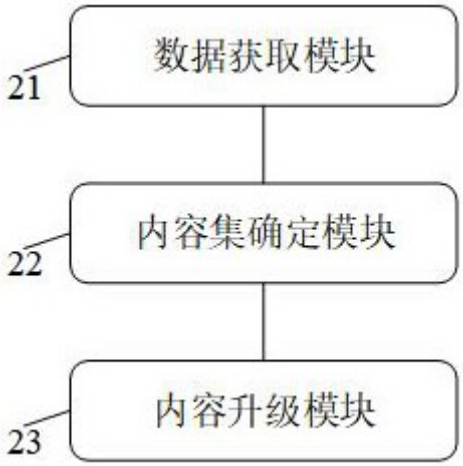

21
数据获取模块
22
内容集确定模块
23
内容升级模块

图2