中文引用格式:盛剑桥,曾丽帆,方圆,等. 基于 IPFS-DEMATEL-ISM 的容器安全威胁关键战术要素研究[J]. 中国安全科学学报,2024,34(6):157-163.

英文引用格式:SHENG Jianqiao,ZENG Lifan,FANG Yuan,et al. Study on key tactical factors of container security threats based on IPFS-DEMATEL-ISM Method[J]. China Safety Science Journal,2024,34(6):157-163.

基于 IPFS-DEMATEL-ISM 的容器安全威胁关键战术要素研究*

盛剑桥[1]工程师, 曾丽帆[2], 方 圆[1]高级工程师, 吴 俊**[2]教授

(1 国网安徽省电力有限公司 信息通信分公司,安徽 合肥 230041;
2 北京邮电大学 经济管理学院,北京 100876)

中图分类号:X944.4;TP309 **文献标志码**:A **DOI**: 10.16265/j.cnki.issn1003-3033.2024.06.0074

资助项目:科技部国家重点研发计划项目(2018YFB1403602)。

【摘 要】 为解决电力能源企业"上云"引发的云原生容器安全威胁问题,提出融合区间毕达哥拉斯模糊集(IPFS)、决策试验与评价实验室(DEMATEL)和解释结构模型法(ISM)识别容器安全关键战术要素。首先,基于 IPFS 提取安全专家对容器入侵威胁战术要素的经验判断,其次,应用 DEMATEL 和 ISM 识别容器安全威胁的关键战术要素及要素间的层级拓扑关系。结果表明:持久化和权限提升2个战术阶段的中心度和原因度较高,在整个云原生安全威胁体系中居于核心地位,这2个阶段的安全攻击行为需持高优先级关注;执行和持久化战术阶段的威胁攻击是云原生容器安全的本质要素,初始访问、窃取凭证以及横向移动战术阶段的威胁最直接影响云原生容器安全。研究提出的 IPFS-DEMATEL-ISM 法相较 DEMATEL-ISM 和集成三角模糊数的 DEMATEL-ISM 法在识别容器安全威胁关键战术要素时具有更好区分度和简约解释性。

【关键词】 区间毕达哥拉斯模糊集(IPFS); 决策试验与评价实验室(DEMATEL); 解释结构模型(ISM); 容器安全威胁; 关键战术要素

Study on key tactical factors of container security threats based on IPFS-DEMATEL-ISM Method

SHENG Jianqiao [1], **ZENG Lifan** [2], **FANG Yuan** [1], **WU Jun** [2]

(1 Information and Communication Branch, State Grid Anhui Electric Power Co., Ltd., Hefei Anhui 230041, China; 2 School of Economics and Management, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: In order to address the increasingly serious cloud-native container security threats arising from large-scale cloud migration of systems, the ISM method merging IPFS, DEMATEL, and method were proposed to identify the key tactical factors influencing cloud-native container security threats and their hierarchical logical relationships from the security intruder perspective. The findings of this research are as

* 文章编号:1003-3033(2024)06-0157-07; 收稿日期:2023-12-16; 修稿日期:2024-03-21

** 通信作者:吴 俊(1978—),男,安徽合肥人,博士,教授,主要从事前沿技术创新与大数据分析等方面的研究。E-mail: wujun1127@126.com。

follows: the centrality and causality of the persistence and privilege escalation tactical phases are high, positioning them at the core of the entire cloud-native security threat landscape. Security attacks during these two phases require high-priority attention. Threat attacks during the execution and persistence tactical phases constitute essential factors in cloud-native container security. The threats during the initial access, credential theft, and lateral movement tactical phases have the most direct impact on cloud-native container security. In comparison with traditional and triangular fuzzy sets improved DEMATEL-ISM, our proposed method has better performance in identifying container security-related critical factors.

Keywords: interval pythagorean fuzzy set (IPFS); decision-making trial and evaluation laboratory (DEMATEL); interpretative structural modeling (ISM); container security threats; critical tactical factors

0 引 言

2020 年 4 月,国家发展改革委协同中央网络和信息化办公室印发了《关于推进“上云用数赋智”行动,培育新经济发展实施方案》[1]鼓励广大企业“上云用数赋智”,推动业务创新,加速数字化转型。在此背景下,电力能源企业加快业务应用系统向云端迁移。到 2024 年,将有 15%的应用运行在云端容器中,75%的大型企业将会在生产中使用容器技术[2]。

一般认为,狭义概念的云原生指使用 Docker 软件封装,基于 Kubernetes 平台对容器动态编排管理,采用微服务架构的应用系统。相较于传统的信息系统,云原生应用系统的微服务之间独立自治,互相解耦[3]。广义的云原生是包含系列技术体系、系统设计理念、组织管理方法的全面应用系统变革,核心要素包括基础设施云原生、业务云原生、管理运维云原生,代表技术包括容器、微服务、开发运维一体、持续集成(部署)等[4]。发展云原生的主要目标是支持各类组织在新型动态环境中快速构建和稳定运行可弹性伸缩的应用。由此带来企业应用形态的 2 大变化:①云原生技术给应用带来更好的韧性、适用性、故障自愈率;②遵循微服务设计的应用云原生化,使得应用数量快速增长,应用更为分散,配置更为复杂,应用间交互引发应用接口数量指数级增长,给云原生应用和业务运营的稳定带来新的风险。

容器技术是云原生的基础,既有研究指出,容器遭遇的安全威胁既表现为来源多样,如镜像源不安全[5],环境存在漏洞[6-7],交付机制存在隐患[8]等,也体现为攻击手段各异,如逃逸攻击[5]、拒绝服务攻击[9]等。现有研究多将容器安全威胁视为孤立因素[10-12],不仅较少考虑威胁间的关联关系,还十分缺乏针对电力能源大型企业容器安全的针对性分析。

为应对传统企业“上云”引发的容器安全威胁,笔者拟基于国内某云原生安全服务提供商的项目实践,收集大量针对云上安全威胁及攻击的实例,围绕云原生业务场景,全方面分析攻击者战术与手段,并从云原生容器安全攻防的 8 个战术阶段要素入手,应用区间毕达哥拉斯模糊集(Interval Pythagorean Fuzzy Set,IPFS)、决策实验室(Decision-Making Trial and Evaluation Laboratory, DEMATEL)和解释结构模型法(Interpretative Structural Modeling, ISM),揭示关键战术要素以及要素间的层次逻辑关系,以期识别风险,有效保障云上资产安全。

1 容器安全威胁建模

1.1 容器安全威胁的系统解耦

如果把云原生容器安全防护视为一个复杂系统,可以看到,影响该复杂系统的要素众多且关联。首先,借鉴国外基于真实安全攻防事件总结形成的对抗战术和技术通用知识库(Adversarial Tactics Techniques and Common Knowledge, ATT&CK),找到攻击者典型战术的划分依据[12-13];其次,参考国内公开的容器攻防战术阶段划分;进一步地,针对国内大型电力能源企业总结的 8 类容器攻击典型战术,从入侵者视角出发,识别容器安全的关键战术要素。为量化专家的主观语义评价,识别核心主导要素,展现要素间的层级关系,综合采用 IPFS、DEMATEL 和 ISM 的组合方法展开研究。

1.2 容器安全威胁战术要素的系统建模

从直觉模糊集拓展而来的毕达哥拉斯模糊集法由 YAGER[14]提出,约定毕达哥拉斯模糊集的隶属度和非隶属度平方和≤1。为解决实际决策应用中评价指标属性的隶属度和非隶属度难以用精确数字表征的不足[15],ZHANG XiaoLu[16]提出 IPFS 概念,

采用区间形式来表达评价者的主观评价和偏好。首先采用 IPFS 将专家的语义评价转换为量化分值,以解决专家评分不确定性高难题。DEMATEL 和 ISM 法擅于发现复杂系统构成要素的重要性及要素间层级关系[17-19],文中将 IPFS、DEMATEL 与 ISM 法联合用于研究情境,有利于增强专家经验区分度,识别并可视化展现影响容器安全威胁的表层、过渡和根本因素,方法应用与建模流程如图 1 所示。

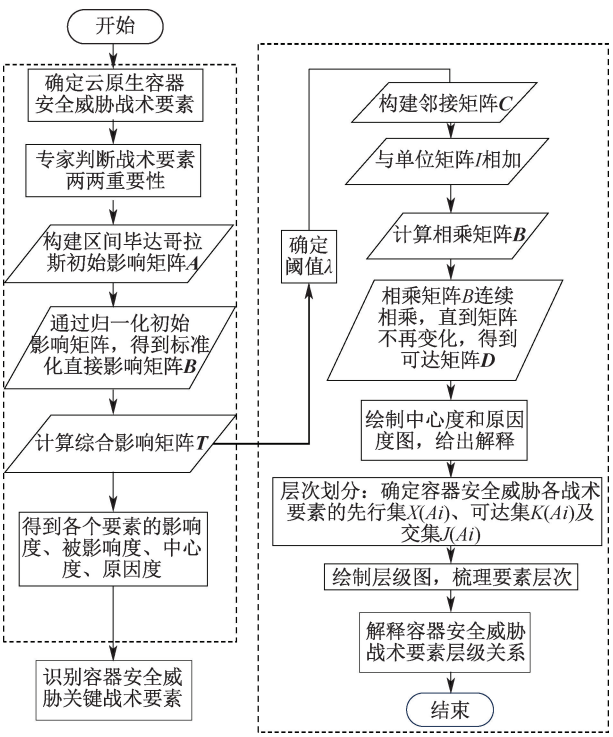

图 1　基于 IPFS-DEMATEL-ISM 建模分析云原生容器安全威胁的流程

Fig. 1　Modeling and analyzing cloud-native security threats based on IPFS-DEMATEL-ISM

实施 IPFS、DEMATEL 和 ISM 法有如下 7 个步骤:

步骤 1:基于国内外文献和企业最佳实践梳理,邀请云原生安全领域专家,确定云原生安全威胁的分析视角、思路与关键要素。

步骤 2:编写问卷邀请领域专家评价云原生安全威胁不同战术之间的两两影响程度,设定为无影响、低影响、中影响、高影响、极高影响。

步骤 3:回收问卷数据,构建区间毕达哥拉斯初始直接影响矩阵 $\boldsymbol{A}=[a_{ij}]_{n\times n}$ (n 为影响要素数量),a_{ij} 表示要素 i 对要素 j 的影响程度,对角线 a_{ij} 表示要素对自身的影响,取值为 0,见下式。其中,$\tilde{p}$ 为区间毕达哥拉斯模糊数,a,b 为区间隶属度,c,d 为区间非隶属度,参照文献[20],设置语义变换见表 1。

表 1　IPFS 的语义变换

Table 1　Transformation of IPFS

语言评价	IPFS 数值
极高影响	([0.80,0.95],[0.00,0.10])
高影响	([0.60,0.80],[0.10,0.30])
中影响	([0.40,0.60],[0.30,0.50])
低影响	([0.20,0.40],[0.50,0.70])
无影响	([0.00,0.20],[0.70,0.90])

$$\tilde{p}=([a,b],[c,d]) \tag{1}$$

$$\pi_-^2=1-(b^2+d^2) \tag{2}$$

$$\pi_+^2=1-(a^2+c^2) \tag{3}$$

$$D(\tilde{p})=(a^2+b^2+(1-c^2-\pi_+^2)+(1-d^2-\pi_-^2)+ab+\sqrt[4]{(1-c^2-\pi_+^2)\times(1-d^2-\pi_-^2)})/x \tag{4}$$

式中:π_-^2、π_+^2 分别为犹豫度下限和上限平方;$D(\tilde{p})$ 为区间模糊数去模糊化后的对应值。

步骤 4:计算标准化直接影响矩阵 $\boldsymbol{B}=[b_{ij}]_{n\times n}$ 和综合影响矩阵 $\boldsymbol{T}=[t_{ij}]_{n\times n}$,$\boldsymbol{E}$ 为单位矩阵,见下式:

$$\boldsymbol{B}=\boldsymbol{A}/x \tag{5}$$

$$x=\max\left[\max_{1\leqslant i\leqslant n}\sum_{i=1}^{n}a_{ij},\max_{1\leqslant j\leqslant n}\sum_{j=1}^{n}a_{ij}\right] \tag{6}$$

$$\boldsymbol{T}=\boldsymbol{B}(\boldsymbol{E}-\boldsymbol{B})^{-1} \tag{7}$$

步骤 5:计算中心度 M_i 和原因度 R_i 并绘制因果图。d_i 为因素 i 的影响度,即直接或间接影响其他因素程度的总和,c_i 表示因素 i 的被影响度,即被其他因素影响程度的总和,见下式:

$$d_i=\sum_{i=1}^{n}t_{ij} \tag{8}$$

$$c_i=\sum_{j=1}^{n}t_{ij} \tag{9}$$

$$M_i=d_i+c_i \tag{10}$$

$$R_i=d_i-c_i \tag{11}$$

步骤 6:构建邻接矩阵 $\boldsymbol{C}=[c_{ij}]_{(n+1)\times(n+1)}$ 和可达矩阵 $\boldsymbol{D}=[d_{ij}]_{(n+1)\times(n+1)}$,见下式。设置阈值 λ 剔除一些影响程度较小的要素,λ 取值通常为矩阵各要素均值与标准差之和[21],同时也可根据研究问题与情境调试决定。

$$c_{ij}=\begin{cases}0, & c_{ij}<\lambda\\ 1, & c_{ij}\geqslant\lambda\end{cases}\quad i,j=1,2,\cdots,n+1 \tag{12}$$

$$\boldsymbol{D}=(\boldsymbol{C}+\boldsymbol{E})^{n+2}=(\boldsymbol{C}+\boldsymbol{E})^{n+1}\neq(\boldsymbol{C}+\boldsymbol{E})^{n}\neq\boldsymbol{C}+\boldsymbol{E} \tag{13}$$

步骤 7:划分 ISM 层级,构建层级图。将要素分别记为 S_1-S_n,依据可达矩阵 $\boldsymbol{D}$ 计算递阶层级要素

集合 $R(S_k)$、$A(S_k)$、$C(S_k)$、$B(S_k)$和 $E(S_k)$，$k=1,2,\cdots,n$，见下式：

$$R(S_k)=\{s_k \in S \mid m_{kj}=1\} \tag{14}$$

$$A(S_k)=\{s_k \in S \mid m_{jk}=1\} \tag{15}$$

$$C(S_k)=R(S_k) \cap A(S_k) \tag{16}$$

$$B(S_k)=\{s_k \in S \mid A(S_k)=C(S_k)\} \tag{17}$$

$$E(S_i)=\{s_i \in S \mid R(S_i)=C(S_i)\} \tag{18}$$

2　容器安全威胁关键战术要素研究

2.1　IPFS-DEMATEL-ISM 建模过程与结果

邀请云原生容器安全领域的15名专家，包括云原生安全提供商2位技术总监、2位高级专家、2位项目经理；电力行业云原生应用厂商2名业务部门负责人、2名高级工程师、2名业务骨干，以及从事云原生安全研究的教授1名、副教授2名。采用问卷方式，调研专家对云原生容器安全威胁不同阶段的主要攻击技术以及各阶段两两间的相互影响。针对问卷结果，使用SPSS. 25. 0对15位专家的评分进行信度检验，发现Cronbach′s α 为0. 872，大于0. 80，说明专家研判结果信度较高。

接下来，将15位专家的语义评价通过表1及式(1)—式(4)转化为区间毕达哥拉斯初始直接影响矩阵 $\boldsymbol{A}$，见表2。

然后，依据式(5)—式(7)计算得到综合影响矩阵 $\boldsymbol{T}$，见表3。

进一步，应用式(8)—式(11)计算输出各阶段的影响度、被影响度、中心度及原因度见表4，此外，绘制各阶段的中心度-原因度散点如图2所示。

表2　初始直接影响矩阵 *A*

Table 2　Initial direct influence matrix *A*

阶段	初始访问	执行	持久化	权限提升	防御绕过	窃取凭证	探测	横向移动
初始访问	0. 000	0. 625	0. 397	0. 245	0. 152	0. 152	0. 152	0. 152
执行	0. 152	0. 000	0. 625	0. 397	0. 397	0. 397	0. 245	0. 152
持久化	0. 152	0. 152	0. 000	0. 853	0. 625	0. 625	0. 245	0. 245
权限提升	0. 152	0. 152	0. 152	0. 000	0. 853	0. 625	0. 397	0. 245
防御绕过	0. 152	0. 152	0. 152	0. 152	0. 000	0. 397	0. 625	0. 245
窃取凭证	0. 152	0. 152	0. 152	0. 152	0. 152	0. 000	0. 625	0. 397
探测	0. 152	0. 152	0. 152	0. 152	0. 152	0. 152	0. 000	0. 853
横向移动	0. 152	0. 152	0. 152	0. 152	0. 152	0. 152	0. 152	0. 000

表3　综合影响矩阵 *T*

Table 3　Comprehensive influence matrix *T*

阶段	初始访问	执行	持久化	权限提升	防御绕过	窃取凭证	探测	横向移动
初始访问	0. 110	0. 332	0. 301	0. 290	0. 300	0. 303	0. 296	0. 280
执行	0. 183	0. 161	0. 378	0. 369	0. 420	0. 426	0. 371	0. 343
持久化	0. 203	0. 234	0. 206	0. 505	0. 525	0. 529	0. 451	0. 417
权限提升	0. 179	0. 207	0. 226	0. 203	0. 508	0. 459	0. 439	0. 386
防御绕过	0. 145	0. 168	0. 183	0. 206	0. 185	0. 315	0. 405	0. 312
窃取凭证	0. 140	0. 161	0. 176	0. 198	0. 226	0. 179	0. 374	0. 341
探测	0. 135	0. 156	0. 170	0. 191	0. 218	0. 221	0. 179	0. 442
横向移动	0. 110	0. 127	0. 139	0. 155	0. 177	0. 180	0. 186	0. 132

表4　云原生容器安全攻击各阶段 DEMATEL 计算结果

Table 4　DEMATEL calculation results of cloud-native container security attack stages

攻击阶段	影响度	被影响度	中心度	中心度排序	原因度	原因属性
初始访问	2. 212	1. 206	3. 418	8	1. 006	原因要素
执行	2. 670	1. 548	4. 218	6	1. 121	原因要素
持久化	3. 071	1. 779	4. 850	1	1. 293	原因要素
权限提升	2. 598	2. 117	4. 715	2	0. 481	原因要素
防御绕过	1. 920	2. 569	4. 478	3	−0. 639	结果要素
窃取凭证	1. 804	2. 612	4. 416	4	−0. 807	结果要素
探测	1. 713	2. 731	4. 445	5	−1. 018	结果要素
横向移动	1. 206	2. 643	3. 849	7	−1. 436	结果要素

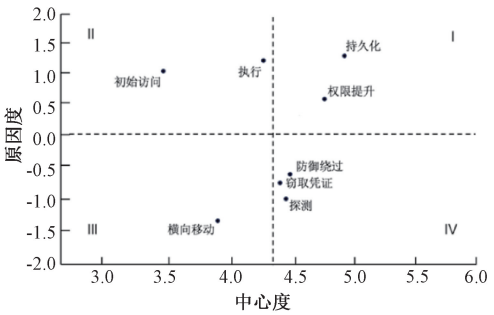

图 2　中心度–原因度散点图

Fig. 2　Centrality-reasoning degree scatter plot

表 4 和图 2 中,中心度越高,表示该要素在系统中的作用越关键,核心程度越强。原因度越高,表示该要素对其他要素的影响越大。原因度大于 0 的因素称为原因因素,原因度小于 0 的因素称为结果因素。从表 3 和图 2 不难发现,中心度排名前 3 的阶段分别为持久化、权限提升和防御绕过阶段,说明这 3 个阶段的安全威胁最关键,处于核心地位;原因度排名前 3 的阶段分别为持久化、执行和初始访问阶段,表明这 3 个阶段对其他阶段的影响最大。另外,防御绕过、窃取凭证、探测以及横向移动阶段均为结果因素,反映这些阶段易受其他阶段的攻击威胁影响。从图 2 可以看出,居于第一象限的持久化和权限提升阶段的中心度和原因度均较高,在整个云原生安全威胁体系中居于核心地位,这 2 个阶段的安全攻击行为需持高优先级关注。

为输出各要素的层级结构关系,计算可达矩阵;为剔除两两影响程度较小的要素,引入阈值 λ,参考已有研究[17,22],分别设置 λ 值为 0.29、0.33、0.38 和 0.43 不同阈值下节点度的衰减情况,如图 3 所示。可以看到,当 λ 取值 0.38 时,节点度较为适中。按照式(12)、式(13)计算,得到可达矩阵 $\boldsymbol{D}$,见表 5。

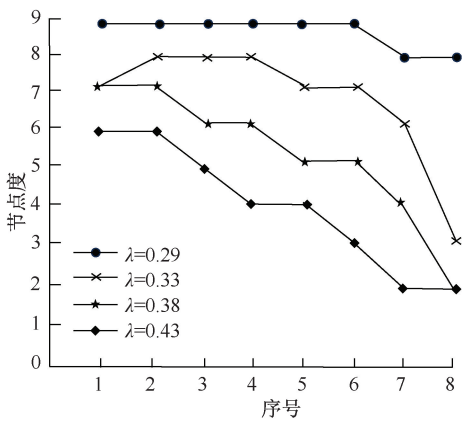

图 3　不同阈值 λ 对应节点度衰减散点图

Fig. 3　Scatter plot of node degree decay corresponding to different threshold values λ

表 5　可达矩阵 *D*

Table 5　Reachability matrix *D*

阶段	初始访问	执行	持久化	权限提升	防御绕过	窃取凭证	探测	横向移动
初始访问	1	0	0	0	0	0	0	0
执行	0	1	0	0	1	1	0	0
持久化	0	0	1	1	1	1	1	1
权限提升	0	0	0	1	1	1	1	1
防御绕过	0	0	0	0	1	0	1	0
窃取凭证	0	0	0	0	0	1	0	0
探测	0	0	0	0	0	0	1	1
横向移动	0	0	0	0	0	0	0	1

根据可达矩阵 $\boldsymbol{D}$ 及式(14)—式(18),进行层次划分,绘制 ISM 层次结构,如图 4 所示。

由图 4 可以看出,执行阶段和持久化阶段的威胁攻击是云原生容器安全的本质要素,它们通过与其他层次要素联系,起着牵一发动全身的根本影响,需要对这 2 个阶段的攻击防御高度重视。权限提升、防御绕过和探测阶段属于中间过渡要素,起着与本质要素和表层要素的跨层影响作用。初始访问、窃取凭证以及横向移动阶段的威胁是表层要素,最直接影响云原生容器安全。其中,初始访问不受其他要素的影响,在层次模型中活跃性较低。窃取凭证和横向移动受到本质和中间过渡要素影响,可控性最强。

2.2　IPFS-DEMATEL-ISM 稳健性验证

为验证提出的 IPFS-DEMATEL-ISM 法性能优势,将传统的 DEMATEL-ISM 法和纳入三角模糊数的 Fuzzy DEMATEL-ISM 法应用同样数据,作试验对比,3 种方法计算输出的中心度–原因度散点图如图 5 所示。

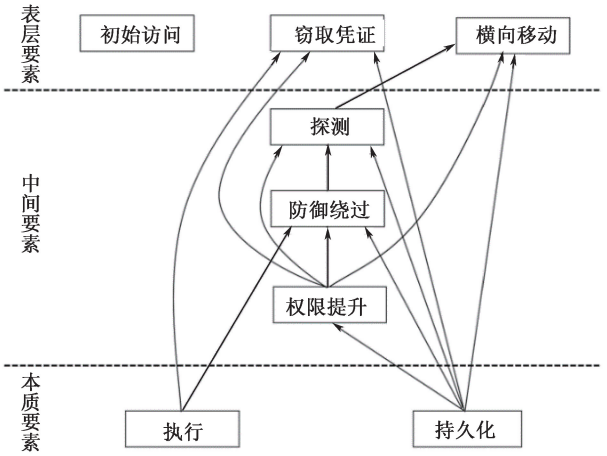

图 4　ISM 层次划分模型

Fig. 4　ISM hierarchy segmentation model

可以看到,文中提出的 IPFS-DEMATEL-ISM 法输出数据点的中心度较为分散,传统的 DEMATEL-ISM 法和 Fuzzy DEMATEL-ISM 法输出数据点的中心度比较集中,不易区分各点间的差异。

此外,采用 Fuzzy DEMATEL-ISM 和传统 DEMATEL-ISM 法构建的综合影响矩阵,接近阈值 λ 的数据点(分别有 14 和 15 个)也多于 IPFS-DEMATEL-ISM 法处理的综合影响矩阵。这些接近阈值 λ 的数据点,在构建可达矩阵时不仅易产生混淆,而且它们所对应边在 ISM 层次化模型中的可解释性相对较弱,影响 ISM 模型的简约性。

综上所述,文中提出的 IPFS-DEMATEL-ISM 法相对另外 2 种方法能更好地区分 8 类容器攻击典型战术间的异同,结果更具稳健性。

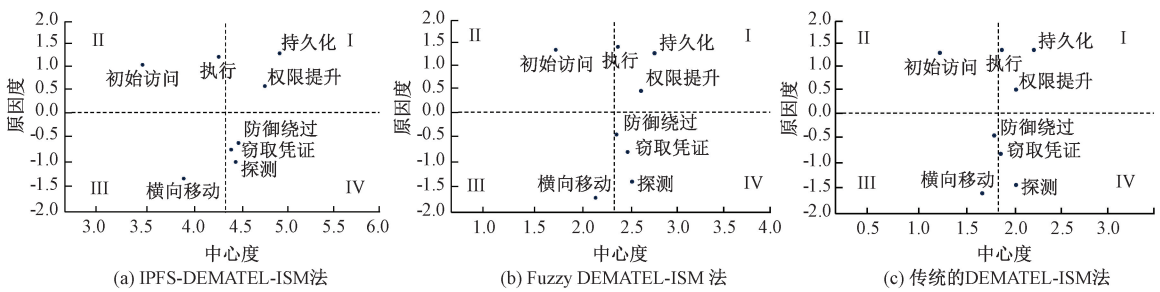

图 5　3 种方法计算输出的中心度-原因度散点图对比

Fig. 5　Comparison of centrality-reasoning scatter plots in three methods

3　结　论

1) 提出 IPFS-DEMATEL-ISM 法,研究表明:持久化和权限提升战术阶段的中心度和原因度较高,在整个云原生安全威胁体系中居于核心地位,这 2 个阶段的安全攻击行为需持高优先级关注。执行和持久化战术阶段的威胁攻击是云原生容器安全的本质要素,初始访问、窃取凭证以及横向移动战术阶段的威胁最直接影响云原生容器安全。

2) 相较于传统和考虑三角模糊数的 DEMLAT-ISM 法,文中提出的 IPFS-DEMATEL-ISM 法能够更好地区分容器安全威胁战术要素间关系,并具有简约解释性。

3) 提出完善企业核心系统上云触发的容器安全威胁应对策略包括将识别的云原生安全攻击关键战术要素与对应的技术手段相勾稽,构建分层分级的安全防御策略;鉴于云原生容器安全威胁复杂,攻防交互多变,企业应选型采纳成熟的一体化云原生安全解决方案。

4) 未来研究可从每个战术阶段下的典型攻击技术入手,进一步分析不同攻击技术对容器镜像内容依赖、执行配置依赖和动态构建依赖的影响,不断完善企业上云引发的容器安全威胁应对策略。

参 考 文 献

[1] 国家发展改革委, 中央网信办. 关于推进"上云用数赋智"行动培育新经济发展实施方案[EB/OL]. [2020-04-07]. https://www.gov.cn/zhengce/zhengceku/2020-04/10/content_5501163.htm.

[2] Gartner Research. Forecast analysis: container management (software and services), worldwide[EB/OL]. [2020-05-29]. https://www.gartner.com/en/documents/3985796.

[3] RAHAMAN M S, ISLAM A, CERNY T, et al. Static-analysis-based solutions to security challenges in cloud-native systems: systematic mapping study[J]. Sensors, 2023, 23(4):1-27.

[4] 胡俊,李漫. 容器安全解决方案探讨与研究[J]. 网络空间安全, 2018,9(12):105-113.
HU Jun, LI Man. Discussion and research on container security solutions [J]. Cyberspace Security, 2018,9(12):105-113.

[5] 任兰芳,庄小君,付俊. Docker 容器安全防护技术研究[J]. 电信工程技术与标准化, 2020,33(3):73-78.

REN Lanfang, ZHUANG Xiaojun, FU Jun. Technical research of docker container security protection [J]. Telecom Engineering Technics and Standardization, 2020,33(3):73-78.
[6] 杨长茂,冯超,谷晓剑. 云原生中的容器安全防护和实践[J]. 保密科学技术, 2021(1):36-42.
[7] 宋胜攀,刘振慧,庄东燃. 开源容器技术安全分析[J]. 保密科学技术, 2021(1):29-35.
[8] 边曼琳,王利明. 云环境下 Docker 容器隔离脆弱性分析与研究[J]. 信息网络安全,2020,20(7):85-95.
BIAN Manlin, WANG Liming. Analysis and research on vulnerability of docker container isolation in cloud environment [J]. Netinfo Security, 2020,20(7): 85-95.
[9] 邢云龙,严飞,刘彦孝,等. 基于系统调用限制的容器安全防护方案[J]. 武汉大学学报:理学版,2022,68(1):35-43.
XING Yunlong, YAN Fei, LIU Yanxiao, et al. Container security protection scheme based on system call restriction [J]. Journal of Wuhan University:Natural Science Edition, 2022,68(1):35-43.
[10] 周大成,陈鸿昶,何威振,等. 基于深度强化学习的微服务多维动态防御策略研究[J]. 通信学报,2023,44(4):50-63.
ZHOU Dacheng, CHEN Hongchang, HE Weizhen, et al. Research on multidimensional dynamic defense strategy for microservice based on deep reinforcement learning [J]. Journal on Communications, 2023,44(4):50-63.
[11] 夏懿航,张志龙,王木子,等. 基于依赖关系的容器供应链脆弱性检测方法[J]. 信息网络安全,2023,23(2):76-84.
XIA Yihang, ZHANG Zhilong, WANG Muzi, et al. Dependency-based vulnerability detection method in container supply chain [J]. Netinfo Security, 2023, 23(2): 76-84.
[12] 王海林,颜颖,唐旭玥. ATT&CK 在安全运营中的应用研究[J]. 网络安全技术与应用,2022(8):5-6.
[13] 张宇翔,韩久江,刘建,等. ATT&CK 框架下基于事件序列关联的网络高级威胁检测系统[J]. 计算机科学,2023,50(增 1):710-716.
ZHANG Yuxiang, HAN Jiujiang, LIU Jian, et al. Network advanced threat detection system based on event sequence correlation under ATT&CK framework [J]. Computer Science, 2023,50(S1):710-716.
[14] YAGER R R. Pythagorean membership grades in multicriteria decision making[J]. IEEE Transactions on Fuzzy Systems, 2013,22(4):958-965.
[15] ATANASSOV K T. Intuitionistic fuzzy sets [J]. Fuzzy Sets and Systems,1986,20(1):87-96.
[16] ZHANG XiaoLu. Multicriteria Pythagorean fuzzy decision analysis: a hierarchical QUALIFLEX approach with the closeness index-based ranking methods[J]. Information Sciences,2016,330:104-124.
[17] 李广利,严一知,刘文琦,等. 基于 DEMATEL-ISM 的矿工不安全情绪形成因子研究[J]. 中国安全科学学报,2021,31(7):30-37.
LI Guangli, YAN Yizhi, LIU Wenqi, et al. Research on formation factors of miners´ unsafe emotions based on DEMATEL-ISM [J]. China Safety Science Journal, 2021,31(7): 30-37.
[18] 缪秀梅,陈烨天,米传民. 基于 ISM 和在线评论的汤山温泉顾客满意度研究[J]. 中国管理科学,2019,27(7):186-194.
MIAO Xiumei, CHEN Yetian, MI Chuanmin. Study on consumer satisfaction of tangshan hot springs based on ISM and online reviews [J]. Chinese Journal of Management Science, 2019,27(7):186-194.
[19] 赵希男,肖彤. 基于模糊 DEMATEL-ISM 方法的员工绿色行为影响因素研究[J]. 科技管理研究,2021,41(5):195-204.
ZHAO Xi´nan, XIAO Tong. Research on factors influencing employee´s green behavior based on fuzzy-DEMATEL-ISM method [J]. Science and Technology Management Research, 2021,41(5):195-204.
[20] YU Shuaiju,GENG Xiuli,HE Jianjia, et al. Evolution analysis of product service ecosystem based on interval Pythagorean fuzzy DEMATEL-ISM-SD combination model[J]. Journal of Cleaner Production,2023,421:1-17.
[21] 郝江锋,陈华友,钱云,等. 基于区间值毕达哥拉斯模糊数的多属性决策方法[J]. 重庆工商大学学报:自然科学版,2020,37(3):88-93.
HAO Jiangfeng, CHEN Huayou, QIAN Yun, et al. Multi-attribute decision making method based on interval value pythagoras fuzzy number [J]. Journal of Chongqing Technology and Business University:Natural Science, 2020,37(3):88-93.
[22] 张勇,王祥宇. 基于 DEMATEL-ISM-BN 的施工人员不安全行为致因研究[J]. 中国安全生产科学技术,2020,16(11):110-116.
ZHANG Yong, WANG Xiangyu. Study on causes of unsafe behaviors of construction workers based on DEMAREL-ISM-BN[J]. Journal of Safety Science and Technology, 2020,16(11):110-116.

作者简介: 盛剑桥 (1992—),男,安徽合肥人,硕士,工程师,主要从事电网信息系统安全研究等方面的研究。E-mail: cambridgeace@ sina. com。