

订阅DeepL Pro以编辑此演示文稿。  
访问[www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document)，了解更多信息。

BEAM：基于异常的企业多域数据威胁检测系统

摘要--组织面临着不断增加的安全威胁风险。安全威胁是多方面的，给防御者带来不同程度的挑战。

虽然传统的确定性签名和基于相关性的方法作用有限，但基于行为的异常检测方法最适合于识别无签名的威胁，如来自外部对手或内部活动的威胁。为企业安全建立异常检测系统的挑战很多。本文介绍了

一个新的异常检测系统，解决了企业中多领域数据的特征工程过程，并提供了一个基于贝叶斯的信息风险评分方法

融合。该系统对动态的用户和网络行为具有适应性，并通过设计产生可解释的结果。

为了对没有已知标记的攻击数据的基线系统进行定量评估，我们提出了一种合成地面真相的方法，以证明改进的效果。

在检测性能方面。

1.绪论

组织面临着来自安全威胁的不断增加的风险。根据Verizon最近的一份报告[1]，百分之七十的网络攻击是由外部人员实施的，而其中百分之三十的网络攻击涉及内部人员。内部人的威胁尤其难以防范，无论是来自某人利用其合法的数据访问权达到邪恶的目的，还是以违反可接受的用户政策的方式进行网络活动。由于来自内部人员或外部对手的活动是动态的，传统的检测威胁的方法是将数据与已知的数据进行比对。

黑名单上的签名或手工制作的相关规则基本上是无效的或不相关的。近年来，基于行为的异常检测工作已经出现，以解决这些安全威胁；特别是，用户和实体行为分析（UEBA）[2]已经在网络安全行业出现，成为检测行为异常的可行方法。

企业安全产品产生大量不同类别或 "域 "的实体或用户活动数据。活动域的例子包括资产登录和访问、账户管理、VPN、电子邮件、代理/防火墙、云应用、端点和物理访问。由安全信息和事件管理（SIEM）系统处理并存储的事件被用于行为建模，以标记出警报的偏差。建立基于行为的异常检测系统的挑战是多方面的。它们包括一种方法来

本文介绍了基于行为的自适应多域威胁检测系统，包括连续和自适应行为分析的特征、来自不同数据域的行为异常的信息融合策略、近实时处理的需要、对自我解释结果的要求，以及对所建系统进行定量评估的恶意事件标记的基础真相数量实际上是不存在的现实。本文提出了一个基于行为的自适应多域威胁检测系统，称为BEAM，用于实时检测企业网络和用户事件中的安全威胁。特征工程过程是有原则的，并在不同的数据域中变得实用。贝叶斯方法被用来评估用户会话风险的优先级。该系统通过从持续的用户活动中自我更新来进行自我学习。其结果是不言自明的，因为这是一个白盒系统。为了评估，我们引入了一种方法来综合标记的地面真相，以进行定量评估，并将BEAM与另一个依靠精心设计的规则和手动分数调整的基线系统进行比较。

本文的大纲如下。第2节提供背景和相关工作。第3节描述了该系统从特征推导过程到基于贝叶斯的风险评分机制。第4节描述了数据集、评估程序和实验结果。我们在第5节中得出结论。

2.相关工作

利用基于行为的方法的安全威胁检测系统使用来自各种领域的数据来检测恶意活动。虽然存在商业化的系统[3][4][5]，但基于行为的威胁检测仍然是一个具有挑战性的问题，而且基本上没有得到解决。过去Eldardiry等人的学术工作[6]发现了在各数据域表现出不一致行为的异常用户。它从所有其他领域的集群指数中预测出一个用户在一个领域中的潜在的同伴集群指数。我们的工作不是识别用户的异常，而是识别单个用户会话的异常，更适合于安全中心的运作。Bose, et al., [7]详细介绍了一个基于Spark流的异常检测的架构。它一次性建立了所有领域的特征，并使用k-近邻算法进行基于用户和角色的异常检测。作品[8]也是一个基于流的系统，采用聚类的方式来寻找局部的异常值。Zargar.等人，[9]对数据条目采取了一种知识诊断的方法。主要的假设是，如果一个用户表现出某种行为，比如出现自己历史上未知的新数据条目，而这种行为是另一个用户在不同的数据通道中所独有的，则对其发出警报。上述系统没有考虑从用户反馈中持续学习。

Veeramachaneni.等人，[10]在应用监督学习进行分类之前，通过深度学习和矩阵分解来提取特征。Tuor, et al., [11] 使用深度神经网络（DNNs）和循环神经网络（RNNs）的变体来识别每个网络用户的不特征的活动。Liu.等人，[12]使用深度自动编码器来检测内部人的威胁。Yen.等人，[13]在通过主成分分析（PCA）进行特征提取后，应用K-means来寻找离群的主机。Shyu.等人，[14]也同样使用PCA进行特征提取来进行离群者检测。诸如此类的黑盒系统不可避免地缺乏输出警报的可解释性--这是对可操作结果的关键要求。

Maloof.等人，[15]使用一个由布尔随机变量组成的三层树状贝叶斯网络作为特征。Gheyas[16]比较了一些内部威胁检测系统，显示研究界对基于贝叶斯的学习算法有偏好。我们采用贝叶斯方法是因为它有很多优点。

3.BEAM系统设计

BEAM是一个基于行为的自动化异常检测系统，用于企业级安全威胁检测。影响其设计决策的因素有以下几点。

\_系统的结果必须是可以自我解释的。这是对安全操作中心的一个重要要求。可操作的安全警报始于理解

的警报本身。

企业级应用需要近时间的操作。特征提取必须在事件层面上具有计算效率，以便进行实时或接近实时的警报。

\_ 企业增加新的数据域进行监控的情况并不少见。分析师们要求在系统中增加新的异常指标的灵活性。行为建模框架必须是灵活的，以适应数据域的增加和功能的变化。

\_该模型必须适应网络和用户行为的动态性质。用户、对等人和组织层面的资料是不断更新的。

每当有专家或分析师的反馈时，系统必须利用它，并允许有一个路径来纳入人类的输入，以更新模型参数。

BEAM是为了满足上述要求而设计的。在高层次上，在其训练阶段，网络实体被单独剖析，其活动在不同的数据域中被跟踪。(一个网络实体是一个用户，一个用户的同级群体，或整个组织）。)学习特征是按网络事件定义的。它们包括一套丰富的异常检测器和相关背景。因此，一个贝叶斯网络从这些特征中被学习。

在评分阶段，每个用户事件根据其观察到的特征值被分配一个风险分数。在给定的一天中，用户的总体风险是由他们迄今为止看到的所有事件的风险汇总而成的。在任何时候，都有一个评分排名的用户列表可供调查。接下来我们将更详细地描述BEAM。

3.1.数据预处理

企业网络和服务由一系列的安全、网络和服务器基础设施产品支持。支持用户活动领域的示例数据源有：。

微软的活动目录服务：Windows域网络中所有用户和计算机的认证和授权事件

\_ 身份管理产品：用户或计算机账户创建和删除的事件

\_ 网络代理产品：网络活动事件和警报，例如阻止与潜在恶意域或URL的连接

数据丢失预防产品：与数据渗出有关的安全事件的警报

\_VPN产品：虚拟专用网络登录事件，如登录成功或失败

\_ 数据安全产品：数据库活动的事件，如数据库查询

\_ 徽章系统产品：用于物理建筑或门禁的事件

云服务：基于云的应用程序使用的事件或警报

数据域的原始事件可能来自多个供应商的产品，或来自一个供应商的产品（但版本不同）。对数据源进行解析和规范化是非常关键的，这样一来，相同领域的事件--但具有不同的格式--就会被合并和规范化，以达到分析的目的。例如，为了规范用户资产登录和访问领域的事件，Kerberos登录事件是通过合并Windows AD事件ID 4768和672来规范的[17]；远程访问登录事件是Windows事件ID 4769或2624，登录类型3或8；账户创建元事件是Windows事件ID 4720或624。

安全日志数据中的数据解析和规范化需要领域专业知识，是建模前的一个非微不足道的关键步骤。(以下我们把事件称为规范化的事件。) 把领域表示为Cv，其中v是领域索引，1 < = v < = V，其中V是领域的总数。

3.2.风险框架

BEAM有实时的操作要求，即对一天开始以来的用户活动的累积风险进行perevent评分。BEAM定义一个用户活动会话S从24小时的开始到当前时间，但不超过24小时的结束时间。

然后，一个会话由T用户的可观察事件fevt g的集合组成，其中t是事件索引，v是事件所属的域。

我们将整体会话风险定义为一个会话中所有观察到的域的风险RCv之和。

Rtotal =X Cv RCv (1)

其中，域的风险是单个事件级风险fRv et g和域的会话级风险Rv s之和。

RCv = XT t Rv et + \_Rv s (2)

其中α允许对事件级和会议级风险的相对贡献进行一些灵活调整。

3.2.1.事件层面的特征。风险Rv et是基于从域Cv的事件et中得到的特征向量评估的贝叶斯风险。一个事件的特征是异常检测器和上下文的集合。异常检测器表明事件的某一方面或某一数据元素相对于跟踪的行为特征而言是否异常。

简介是对被追踪数据的历史描述，并持续更新。

异常检测器功能。在涉及分类数据的地方，档案是基于时间的，对数据值的最近访问时间进行跟踪。例如，跟踪用户访问的资产的档案由一个资产的图元列表和最近访问的时间戳组成。在涉及数字数据的情况下，档案是通过boxplot方法或参数概率函数对过去的观察值的描述。例如，一个跟踪用户发送的电子邮件大小的配置文件使用boxplot来描述样本的四分位数范围。配置文件所追踪的行为简单易懂，对可解释性很有帮助。BEAM为每个用户的所有领域以及每个用户的同行组和整个组织建立了一套全面的行为档案。一个用户可能属于多个同行组--例如，部门、职称、地理位置以及他们所关联的安全访问组。

异常检测器检查当前的数据项是否被认为是新的，不寻常的，或者是符合概况的异常值。在分类数据的情况下，如果数据是配置文件中的新数据，或者最后一次被看到是在N天之前（N=30在实践中效果很好），异常检测器会返回TRUE。然而，如果有关数据在人口中是新的--例如，在用户第一次访问企业中新部署的资产的情况下--检测器不认为这是一个异常情况。在评估之前，数据必须是成熟的或 "收敛的"。如果数据老化超过M天，我们就说它已经收敛了。(M=5在实践中运作良好)。

在数字数据的情况下，如果它们被认为是在剖析分布中超过某个阈值的离群点，检测器就会返回TRUE。

语境特征。除了异常检测器之外，静态和事实的上下文数据作为事件的特征，用于风险评分。上下文数据可从数据源获得，如LDAP数据库或其他IT操作数据库；例子包括一个用户对某些资产的特权访问状态，或一个资产是工作站还是服务器。

在评估一个事件的风险时，上下文特征的作用是提供上下文，以校准观察异常检测器检测到的异常事件所带来的风险程度。例如，异常检测器监测正在运行异常进程的用户所带来的风险，最好由运行该进程的机器是关键服务器还是工作站来校准。

3.2.2.会话级别的特征。公式2中的风险Rv s是根据会话中域Cv的事件得出的特征向量评估的贝叶斯风险。与事件级特征类似，会话级特征是异常检测器和背景指标的集合。会话中的事件被汇总以建立档案和检测器；例如，在这个会话中传输的字节数，或在这个会话中访问的资产数。

3.2.3.贝叶斯建模。让R表示Rv et或Rv s。

在训练期间，目标是为每个用户的每一个可能的特征向量~ f = (f1; f2; :; fI )学习R，长度为I。在评估期间，R只是根据当前的特征向量进行查询；然后用户的整体会话风险如公式1所示。

我们把R定义为用户对数据是恶意的或者是在特征向量下是高度关注的异常的后验概率。用M表示 "恶意或高度关注的异常情况"，用L表示 "合法或不感兴趣"。

R := P(Mj ~ f) = P( ~ fjM)P(M)

P( ~ fjM)P(M) + P( ~ fjL)P(L) (3)

为了计算P( ~ fjL)，我们假设观察到的历史数据基本上是正常的和合法的，而且就我们的风险推断而言，任何目前的恶意或异常事件的数量都是可以忽略不计的，在统计学上是不重要的。

用于计算用户的P( ~ fjL)的数据是他们的局部充分统计量被人口的全局充分统计量所平滑。

P( ~ fjL) = (1 \_) \_ C0 \_ Countu( ~ f) + \_ \_ Countg( ~ f)

(1 \_) \_ C0 \_ P

~ f0 Countu(~f0) + \_ \_

P

~ f0 Countg(~f0)

其中C0 =

P

~ f0 Countg(~f0)

P

~ f0 Countu(~f0)

(4)

Countu( ~ f) 是指从用户自己的Phistorical会话中观察到特征向量f~的会话的数量。

Countu(~f0)是同一用户历史中所有可能观察到的特征向量的所有此类计数之和。同样，Countg(~f)是观察到特征向量的aPll用户的会话数，而~ f0 Countg(~f0)是整个用户群体中所有可能观察到的特征向量的所有此类计数的总和。

C0是一个比例系数，使局部充分统计量与全局充分统计量的质量1比1相等。\_是一个介于0和1之间的参数，控制人口-全球与用户-本地充分统计的平滑度。

除非专家分配或分析员反馈另有偏好，否则假设可能性P( ~ fjM)在所有观察到的特征向量上是统一的。事实上，贝叶斯推理方案允许专家意见对其进行调整，并允许用户反馈在生产环境中更新P( ~ fjM)。在没有专家知识或分析师反馈的情况下，公式3中的风险只是反映了预测M的特征向量的程度或稀有性或异常性。最后，公式3中的先验P（L）和P（M）被假设为0.5，之前没有假设与L和M有关；这也是基于贝叶斯的垃圾邮件检测软件的做法[18]。

3.2.4.域的独立性。整体会话风险是一个会话中各域风险的总和，如公式1所示。由于整体风险是相加的，这就意味着各域的活动是独立的。例如，我们相信用户在VPN数据域的行为与文件访问数据域是合理独立的。这个假设提高了特征设计的 "模块化"，因为这种特征的变化是局部的。它也提高了随着时间推移增加新领域的可扩展性。表1显示了这项工作所分析的域的例子。

3.2.5.域中特征组的条件独立性。为了计算来自域Cv的风险RCv，给定其特征~ f，必须评估可能性P( ~ fjL)。

虽然有可能直接计算这个可能性，而不考虑~f的大小，但在实践中，最好是利用特征的条件独立性，这样就可以了。

P( ~ fjL) = YJ j=1 P( ~ gj jL)

领域 事件计数 用户计数

账户登录和访问 1916464 2112

账户管理 109 7

申请114866 1664

徽章访问 12 5

数据丢失预防 45482 432

数据库 15724371 21

电子邮件 42950 414

端点 22497648 1019

文件访问 914175 704

网络接入和Aogon 1241288 1999

供应商的提醒 367 37

VPN 378 196

表1:一个企业环境

其中有J个条件独立的组~gj，每个组由~f的一个不重叠的特征子集组成。

表2显示了将VPN领域的事件级特征分配给四个条件独立组的例子。

团体活动层面的特点

第1组

用户的VPN境界异常

用户的对等体的VPN境界异常

用户的目标主机异常

对等组的异常目标主机

第2组

用户的异常源主机

组织的异常源主机

用户异常的操作系统

用户的异常源IP

第3组 用户的异常VPN活动

同行组的VPN活动异常

第4组

登录失败

源IP被列入黑名单

用户是一个承包商或合作伙伴

帐户被禁用

表2：VPN领域的条件独立特征组

将特征组织成独立的组有两方面的好处。首先，对联合似然的估计预计会更稳健。联合特征的总可能性是条件独立的特征组的可能性的乘积；每组有可管理的或较少的特征数量，减少了联合估计大量特征的可能性所带来的数据分裂问题。

更重要的是，将特征结构化为条件独立的组，可以提高结果的可解释性。对于一个高分的环节，系统可以有选择地只呈现对该环节得分有重大贡献的、尺寸较小的关键特征组，而不是呈现整个特征向量~f（尺寸I可能很大）。这就提高了结果的可读性

- 在一个生产系统中，这是一个关键的考虑因素。BEAM尽可能地将异常检测器特征和上下文特征组织到组中。虽然组的设计是一个手动过程，但有一些准则需要遵循。

比如说。

\_ 使用建立在类似数据上的配置文件的异常检测器被归为一组，因为它们不应该是独立的。例如，使用与用户源机器有关的配置文件的检测器被分组在一起。同样地，与用户活动的目标机器有关的异常检测器也被归为一组。

\_ 用户、他们的同行和组织关于类似活动的异常检测器被归为一组，因为它们不是独立的。例如，如果当前的用户事件对该用户的部门概况来说是异常的，那么它对用户本身也一定是异常的，尽管不一定反过来。

如果上下文对校准组中被触发的异常检测器的风险有用，则上下文特征是异常检测器组的一部分。例如，用户是否是管理员的上下文与各种异常检测器分组，检查用户、他们的同行或组织对资产的异常访问。检测器的风险取决于用户是否是管理员。

3.2.6.风险等级的提高。方程3中的会话风险假定所有事件都独立地对会话产生风险，无论它们来自哪个领域。一些领域，或其组合，比其他领域更不经常被观察到。具有来自较少的领域或领域组合的事件的会话，直觉上应该比其他会话的排名高。因此，在会话风险Rtotal上引入一个加权因子以反映基于会话中观察到的领域多样性的排名偏好是很有用的。与Zhou等人的多视图融合工作类似，[19]，我们将每个领域视为会话活动的一个视图。我们引入领域多样性因子WD和相应的加权风险分数RD total。

WD = QV v P(Cv) P(C1;C2;:CV ) RD total = Rtotal \_WD (5)

其中Cv是第v个域，该域中的任何一个异常检测器特征在一个会话中都返回 "true"。WD有一个理想的特性，即当一些领域相互依赖时，它将小于1.0，从而惩罚会话的得分。否则，当域是真正独立的，如它们在一个会话中提供最大的信息，WD将是1.0，从而保持会话得分。

4.实验

4.1.基线系统

BEAM与部署在生产中的基线威胁检测系统进行了比较。后者由一大批大小为N的规则组成，针对这些活动事件进行评估。其第i条规则i是单独制作的，在触发时有一个手动分配的分数Si。用户会话的总风险Stotal是被触发规则的分数之和。

总数=XN I Si (6)

一个规则要么是基于事实的，要么是基于异常的。基于事实的规则只是检查数据是否与某个事实确定匹配；例如，事件的IP地址是否在黑名单上。与BEAM的异常检测器类似，基于异常的规则是根据用户配置文件来评估数据。对于分类数据，配置文件是基于计数的直方图。对于数字数据，配置文件是通过首先将数据聚类为数字范围的仓，在此基础上建立基于计数的直方图。鉴于基于直方图的分布，事件级和会话级的规则都被定义并启用，以便在数据值是新的或不寻常的情况下，根据其对某些阈值的p值触发。最后，一个规则可以有各种手工制作的条件作为其触发要求的一部分；例如，数据必须有一定的背景，或者该规则只能在其他规则的触发状态的条件下触发。表3显示了每个数据域的基线系统的规则数。

基线系统在生产中的表现令人满意，但确实需要针对环境进行大量的开发和调整工作。手工分配的规则分数是基于专家的主观意见。规则的定义有时需要复杂和重叠的条件来保证精度。各种内部参数的调整，包括用于触发基于异常的规则的单个p值阈值，都是非同小可的。此外，规则是根据需要独立开发的；每个规则的范围都很具体，不能泛化。因此，规则的数量会随着时间的推移而增加，而且它们的统计独立性也得不到保证。触发规则的分数相加构成会话分数并不是最佳的。

4.2.数据设置

我们在一个有多个数据源的企业网络环境中评估了BEAM。该环境总共有4,882个用户，120,667个用户会话，以及43,098,903个事件。表1列出了观察到的每个域的事件量。有63天的数据可用于实验。第一个月用于初始化配置文件，然后在整个数据期的其余部分持续更新。第二个月用于收集充分的统计数据，异常检测器将从这些数据中建立P( ~ fjL)。剩下的两天用于打分和评估。

4.2.1.BEAM特征。正如第3.2节中所讨论的，为每个领域设计了事件级特征和会话级特征。条件性的独立特征组被定义。对于特征设计，我们利用了基线系统中的规则信息。我们有效地将规则翻译并规范化为学习特征，但没有增加新的净信息。表3显示了为BEAM设计的所有评估领域的特征和条件独立特征组的数量。特征的数量比一个领域中的规则的数量要小；有时这种数量上的差异是巨大的。例如，只有7个BEAM特征被用来完全捕获与资产登录和访问领域有关的47条规则。与规则相比，配置BEAM的特征所涉及的复杂性较低。

尽管特征的信息表示更紧凑，但特征的组合比规则更有表现力--有时能捕捉到基线规则没有涵盖的数据条件。例如，在资产登录和访问领域的活动中，通常会有以下两个规则：用户规则与异常检测器，检查其用户的资产访问是否异常；用户的同级规则与异常检测器，检查该资产访问对其同级群体是否异常。仅仅是这两条规则并不能捕捉到用户有异常的资产访问，但对他的同侪来说却没有的情况。在BEAM中，由两个异常检测器（每个都输出一个布尔状态）产生的所有四个活动场景都有分数，因此提供了一个完整的风险场景覆盖。

4.2.2.合成的地面真相。除非进行明确的渗透测试工作，否则已知安全威胁数据的地面真相标签实际上是不存在的。为了评估基于异常的威胁检测系统，我们对地面真相进行了如下合成。从评估期间随机抽出两个用户会话列表；它们的用户不重叠。第一个列表中的会话是受害者会话；第二个列表中的会话是攻击者会话。受害者和攻击者的会话是随机配对的。受害者会话通过注入属于攻击者会话的事件而被欺骗。这种被欺骗的受害者会话是合成的，含有受害者用户不知道的异常活动的正标签会话。我们使用这种欺骗的数据集来评估BEAM和基线系统的相对性能。

这个主张是，更成功的、基于异常的威胁检测系统应该更好地将欺骗性会话与非欺骗性会话分开。

评估的范围可以细化，并通过改变欺骗的条件使之更有针对性。我们为两种不同的攻击场景创建了两套合成的地面真相。

\_外部攻击：攻击事件被注入到受害者会话中，没有修改。由于源设备或IP没有被修改，攻击数据看起来就像来自外部对手。

\_内部攻击：攻击事件被修改为与受害者历史中的主导源设备、源IP、目标设备和浏览器的用户代理字符串相匹配。由于攻击活动事件看起来像是来自受害者的正常硬件，因此异常事件看起来像是来自受害者用户本人，从而模仿内部活动。

我们对这两个场景的准确性进行评估。在两天的评估期间，每个场景都有4,533个负面标记的合法会话和1,071个正面标记的攻击会话。

请注意，这种地面真实数据构建方法不应该被用来建立用于操作的准确性报告。相反，它的目的只是为了评估异常检测系统的相对性能差异。

4.3.结果和分析

BEAM和基线系统在外部和内部攻击场景中都进行了评估。图1a显示了外部攻击检测场景下接收器操作特征曲线（ROC）的准确性表现。图1b显示了低假阳性率区域的放大图，在该区域选择了一个合适的阈值进行操作。(该比率是被标记的会话数量与具有非零会话分数的会话数量的比率）。)

例如，在为期两天的测试期间，基线运行中有2,497个会话的分数不为零。2%的假阳性对应于每天约25个标记的会话。

在外部攻击检测场景中，BEAM的表现明显优于基线。在2%的假阳性率下，BEAM的攻击检测率比基线好40%。图1c显示了类似的比较，但针对内部攻击检测场景。在2%的假阳性率下，BEAM的准确性优势在后一种情况下继续保持。

公式4中的参数\_控制了在计算用户的P( ~ fjL)时将用户的局部充分统计量与群体的整体充分统计量进行平滑处理。图2显示了在放大的ROC图中改变这个参数的效果。我们观察到\_ = 1给出了最好的性能，其中局部和全局充分统计量是一对一的，质量相等。此外，仅仅依靠本地统计量而不进行平滑处理，即当\_ = 0时，表现并不好，因为不是所有的用户都有历史数据量来可靠地训练其P( ~ fjL)。

在操作上，多样性因素WD促进了安全操作中心的偏好，即具有更罕见的域组合的会话应该比其他会话排名更高。为了显示其在此应用中的相关效果，涉及更多的域与被触发的异常情况的会话有望排名更高。在那些排名前50位的会议中，图3显示了会议计数与会议中出现异常的域数的直方图。

在这些会议中，我们观察到多样性因素确实导致了更多的会议拥有更多的领域数量。

图4在放大的ROC图中显示了多样性因子的准确性表现。虽然RD total表达了所需的会话排名偏好，但它在提高Rtotal的准确性表现方面也有一点优势。对5的另一个多样性因子的定义是，鉴于会话中存在的域的数量，或V，会话是恶意的概率

W 0 D = P(MjV ) RD0 total = Rtotal \_W0D

虽然RD0总量与RD总量具有相同的预期效果，但RD0

总的来说，在准确性方面表现不佳，因为它没有将域本身考虑在内。

4.4.结论

我们引入了一个基于行为的异常检测系统来检测企业网络数据的威胁。与依赖手工制作的规则和专家确定的评分的普通威胁检测系统相比，BEAM消除了开发和手动调整规则的复杂性。我们概述了它的特征工程过程，并介绍了一个基于贝叶斯的风险评分框架。这个框架在更新风险时很容易容纳专家的偏好和分析员的标签反馈。由于其白盒性质，系统结果具有高度可解释性。最后，我们证明了BEAM在准确性方面比传统的规则驱动的威胁检测系统表现得更好。