CAICT 中国信通院 安恒信息 DAS-security 安全中国

网络安全先进技术与应用发展系列报告

用户实体行为分析技术（UEBA）

（2020 年）

中国信息通信研究院安全研究所

杭州安恒信息技术股份有限公司

2020 年 6 月

版权声明

本报告版权属于中国信息通信研究院安全研究所、杭州安恒信息技术股份有限公司，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院安全研究所、杭州安恒信息技术股份有限公司”。违反上述声明者，本院将追究其相关法律责任。

目 录

一、安全新范式 1
（一）数字化面临的安全挑战 2
（二）新范式破局之道 7
（三）UEBA 的定义与演进 10
（四）UEBA 的价值 13
二、架构与技术 17
（一）基线及群组分析 17
（二）异常检测 18
（三）集成学习风险评分 19
（四）安全知识图谱 19
（五）强化学习 20
（六）其他技术 21
三、部署实施 23
（一）聚焦目标 23
（二）识别数据源与接入数据 23
（三）确定部署模式 24
（四）分析微调与定制 24
（五）迭代优化 25
四、最佳实践 27
（一）专职团队 27
（二）专注于用例开发 27
（三）法律合规性 27
五、典型应用案例 29
（一）恶意内部人员 29
（二）失陷账号 30
（三）失陷主机 32
（四）数据泄露 33

（五）风险定级排序 35
（六）业务 API 安全 36
（七）远程办公安全 37
六、行业应用案例 38
（一）医疗行业 38
（二）金融行业 38
（三）能源行业 39
（四）政务行业 40
七、总结 42
关于 48

图 目 录

图 1 谁是数据泄漏的受害者？ 3
图 2 安全转向数据科学驱动的新范式 8
图 3 SIEM、UEBA、SOAR 的融合趋势 11
图 4 UEBA 的发展现状 12
图 5 典型的 UEBA 系统架构 17
图 6 基线分析与群组分析 18
图 7 孤立森林发现异常点 19
图 8 多种算法进行集成学习 20
图 9 安全知识图谱 20
图 10 UEBA 中的强化学习 21
图 11 UEBA 分析改进与迭代调优循环流程 26
图 12 内部人员导致的安全威胁 29
图 13 内部员工窃取敏感数据场景分析流程图 30
图 14 账号失陷是攻击链模型中的转折点 31
图 15 主机失陷是病毒爆发、勒索软件的前奏 33
图 16 数据泄漏中的攻击移动和数据流 34

表 目 录

表 1　海外市场上的主流 UEBA 厂商分类.....13
表 2　各种安全技术和范式对比.....14

CAICT 中国信通院

一、安全新范式

全球数字化浪潮下，各类信息化成果持续融入亿万大众的生活，也深刻改变着信息技术环境。一方面，以云计算、大数据、物联网、移动互联网等为代表的新技术得到快速应用；另一方面，传统能源、电力、交通等行业平台联入网络，成为关键信息基础设施的有机组成；与此同时，5G 通信、人工智能、区块链等更多颠覆式创新科技已经来到。

以云计算为例，当前，云计算正处于快速发展阶段，技术产业创新不断涌现。其中，产业方面，企业上云成为趋势，云管理服务、智能云、边缘云等市场开始兴起；自 2017 年起，中国公有云市场持续保持高速增长，零售、制造和金融等行业用户对于公有云的接受程度越来越高，公有云在传统行业的渗透率持续提升[1]，云服务在当年的采用率已经达到 70%[2]。

而随着万物互联的到来，边缘计算和物联网（IoT）也蓬勃发展。到 2021 年，边缘托管容器数量将达到 7 亿，企业数据中心之外的工作负载占比 50%，到 2022 年，物联网（IoT）设备数量将达到 146 亿，增强现实（AR）和虚拟现实（VR）的使用量将增长 12 倍，2017 至 2022 年，业务移动流量将每年增加 42%，53%网络安全攻击导致的损失将超过 50 万美元。[3]

[1] 中国公有云发展调查报告（2018 年），中国信息通信研究院，2018 年 8 月
[2] 云计算发展白皮书（2019 年），中国信息通信研究院，2019 年 7 月
[3] 2020 全球网络趋势报告，思科，2020

普华永道和微软中国在 2019 年四季度，联合进行了一次现代化云办公解决方案调研。调研结果发现 81%企业员工在工作中需要在移动设备上使用办公软件，100%企业高管需要使用移动设备进行办公，24%调研对象反映他们每日工作中有超过 30%的任务需使用移动设备在非办公场所完成（比如家中、咖啡厅、机场、火车上、酒店等场所）。预计到 2020 年将有 100 亿台移动设备投入使用，而移动技术的普及正在从根本上改变人们的思考、工作、行动和互动方式。公司已广泛接受自带设备（BYOD）策略，允许或鼓励员工使用其个人移动设备（如手机、平板电脑和笔记本电脑）访问企业数据和系统[4]。2020 年春季一场突如其来的新冠病毒全球大流行，更是让远程办公、移动办公进入了公众视线。

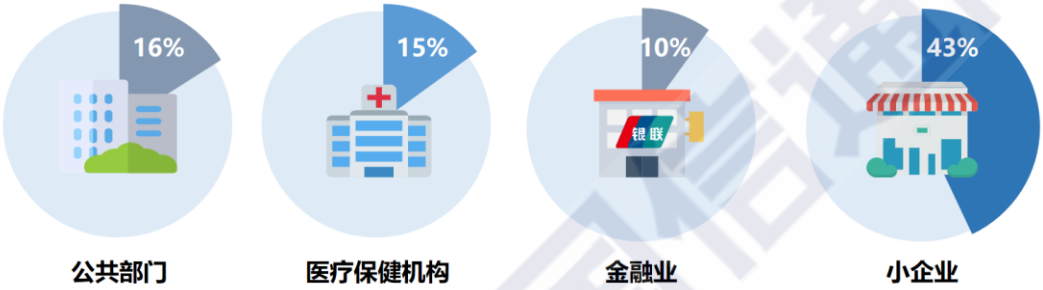
如前所述，数字新时代正在加速全面到来，网络环境变得更加多元、人员变得更复杂、接入方式多种多样，网络边界逐渐模糊甚至消失，同时伴随着企业数据的激增。发展与安全，已成为深度融合、不可分离的一体之两面。在数字化浪潮的背景下，网络信息安全必须应需而变、应时而变、应势而变。

（一）数字化面临的安全挑战

凡有收益，必有代价。数字资产的巨大价值同样被网络犯罪组织所垂涎。2018 年流行的挖矿病毒、勒索软件等安全威胁均以可直接给网络犯罪分子带来经济收益为典型特征，垃圾邮件攻击、移动

[4] 现代化云办公解决方案中国市场白皮书，普华永道和微软中国，2020

安全威胁也处于不断上升趋势。数字化转型促进组织的业务发展的同时，也带来了重大的网络安全挑战。越来越多的敏感数字信息遭受网络攻击被窃取，网络和系统平台被暴露或被操纵，数字资产的保密性、可用性、完整性遭受挑战。网络威胁的影响遍及医疗保健、金融、零售等各行各业，未能采取适当的安全保护举措可能给组织带来巨大的财务和声誉损失。



来源：2019 Data Breach Investigations Report，Verizon

图 1 谁是数据泄漏的受害者？

根据 Verizon 发布的 2019 数据泄露调查报告，如图 1 所示，公共部门、医疗组织、金融机构是数据泄漏的主要受害者，同时大量的数据泄漏事件也波及到了中小型组织[5]。部分原因可能是由于领先组织的安全能力提升，导致一些直接攻击向供应链间接攻击转变。随着最终用户和消费者的安全意识、隐私意识越来越强，对安全事件越来越敏感，每个组织面临的安全事件成本压力也愈加突出。

根据 Ponemon Institute 的报告，基于一项涉及 12 个国家、383 个公司的调查，在 2016 年的数据泄漏的平均代价是 400 万美金，相比 2013 年增长了 29%。2018 年，在美国数据泄漏的平均代价已经达

[5] 2019 Data Breach Investigations Report，Verizon，2019

到了 790 万美金，全世界范围内，每 7 分钟就有一起合规性告警事件发生。[6]IBM Security 在《2019 年度数据泄露成本调研报告》中对 2018 年 7 月至 2019 年 4 月期间的全球 16 个国家和地区的 17 个行业的 507 家公司发生的数据泄露事件进行了调查。调查结果显示，数据泄露事件的全球平均成本为 392 万美元，平均泄露 25575 条记录，每条记录的平均成本为 150 美元，检测和控制数据泄露事件的时间为 279 天。[7]

随着网络犯罪集团的增加和国家隐蔽网络活动的激增，网络攻击在数量和复杂性方面都在增长。网络攻击技术不断升级，网络犯罪分子也在不断提升专业攻击技术，意图突破安全防线，例如，采用非常规文件扩展名、“无文件”组件、数字签名技术、微软 HTML 应用程序（MSHTA）等新技术，躲避安全防护系统的检测与查杀，更好地攻击入侵目标系统。

同时，攻击者也采用了新策略。根据赛门铁克的一份报告，2018 年供应链攻击增长了 78%。据分析 LotL 策略（Living-off-the-Land 攻击，指的是借助系统中已存在的应用程序或工具完成攻击）已成为攻击者最重要的攻击方式之一，旨在协助网络犯罪分子进行复杂攻击时尽量隐藏攻击行为。LotL 技术允许攻击者隐藏在合法进程中，相关攻击事件呈爆发趋势。例如，2018 年恶意 PowerShell 脚本的使用增加了十倍。赛门铁克每月阻止 11.5 万个恶意 PowerShell 脚本，

[6] 2018 Cost of a Data Breach Study，Ponemon Institute LLC，2018
[7] 2019 年度数据泄露成本调研报告，IBM，2019

但不到 PowerShell 总使用量的百分之一。如果阻止全部 PowerShell 脚本将对业务运行产生影响，进一步佐证了 LotL 技术已成为许多高级持续性威胁（APT）攻击团体躲避安全团队检测的首选策略。[8]

外部网络攻击威胁加剧的同时，组织内部及其网络周边的内部威胁也持续增长。网络犯罪分子可能伪装成合法用户，进而突破网络边界、窃取网络凭证、植入恶意软件，或由于组织内部人员工作失误，引发组织内部的网络安全威胁。

根据 IBM X-Force 安全团队的监测，2019 年全球超过 85 亿条记录遭到泄露，相比 2018 年增长超过 200%。究其原因，可能由于内部人员玩忽职守导致数据泄露。由于错误配置的服务器（包括公开访问的云存储、不安全的云数据库以及安全措施不到位的远程同步备份或开放的互联网络区域存储设备）而泄露的记录占 2019 年泄露记录数量的 86%。[9]据外媒报道称，2017 年，美国五角大楼由于在使用亚马逊简单存储服务（S3）时配置错误，意外暴露了美国国防部的机密数据库，其中包含美国当局在全球社交媒体平台中收集到的 18 亿用户的个人信息。[10]

雪上加霜的是，在外部攻击、内部威胁的压力之下，由于数字化时代的信息系统、数字科技越来越复杂，组织和机构脆弱性暴露面也越来越多。

[8] 2019 Internet Security Threat Report，Symantec，2019
[9] X-Force 威胁情报指数，IBM，2020
[10] 五角大楼 AWS S3 配置错误，意外在线暴露包含全球 18 亿用户的社交信息，2017，https://www.sohu.com/a/205831467_354899

根据中国国家信息安全漏洞库（CNNVD）网站数据统计，新增漏洞数量近几年一直保持上升趋势。2018 年，新增漏洞 15040 个，与 2017 年披露的漏洞数量 11097 个相比，增加了 36%。2019 年，国家信息安全漏洞共享平台（CNVD）新收录通用软硬件漏洞数量达 16193 个，与前一年相比同比增长 14.0%，创下历史新高。漏洞影响范围也从传统互联网到移动互联网，从操作系统、办公自动化系统（OA）等软件到虚拟私人网络（VPN）、家用路由器等网络硬件设备，以及芯片、SIM 卡等底层硬件。[11]

因此，安全防护运营团队通常需要跟踪最新漏洞，持续识别网络环境中的隐患，进行加固防护；持续进行安全监控，保持最大的安全可见性，感知全域安全威胁与风险；关注最新的威胁情报，了解最新的攻击组织、技术和方法，持续监控失陷指标（IoC）并应用到威胁检测过程中，同时主动进行威胁狩猎；以及对组织成员进行安全意识教育培训。

但是根据思科的一份调查报告，77%的中型企业发现，从数量繁多的安全解决方案中找出真正有价值的安全警报非常困难。在众多安全警报中，几乎有 46%的警报未经分析验证；54%的警报经过验证后，其中只有将近四成是真实警报，能得到修复的只有不到半数。总体来看，仅不到 10%的告警最终被有效处置。[12]

[11] 2019 年我国互联网网络安全态势综述，国家计算机网络应急技术处理协调中心，2020
[12] 思科 2018 年度网络安全报告，思科，2018

此外，安全团队正在遭受“拒绝服务（DDoS）攻击”。在不对称且长期持久的网络安全攻防对抗形势下，“安全勇士们”责任重大。

总之，组织面临的严峻网络安全挑战来自四个方面：

1. 越来越多的外部攻击，包括被利益驱动或国家驱动的难以察觉的高级攻击；

2. 心怀恶意的内鬼、疏忽大意的员工、失陷账号与失陷主机导致的各种内部威胁；

3. 数字化基础设施的脆弱性和风险暴露面越来越多，业务需求多变持续加剧的问题；

4. 安全团队人员不足或能力有限，深陷不对称的“安全战争”之中。

挑战催生革新，正是在数字化带来的巨大安全新挑战下，安全新范式应运而生。

（二）新范式破局之道

2012 年咨询公司高德纳（Gartner）发表了一份题为《信息安全正在成为一个大数据分析问题》的报告，提出当前信息安全问题正在转变成大数据分析问题，大数据的出现将对信息安全产生深远的影响[13]。在数字时代，安全团队迫切希望通过大数据分析和机器学习，

[13] Information Security Is Becoming a Big Data Analytics Problem，Gartner，2012

提高内部威胁和外部攻击的可见性，提升威胁检测响应能力，成为组织探索将安全分析应用于其网络和其他数据源的关键驱动因素。

安全是人和人攻防对抗的游戏，一切的意图都需要通过行为表达，这是安全运营中最重要也最有价值的一块拼图，同时也是传统方式最欠缺的。传统安全产品、技术、方案，基于单次单点的有限信息，运用签名、规则进行非黑即白式的防护控制，可能导致大量的噪声和误报。虽然已经有告警聚合等基础聚合技术等，尝试修复上述问题，但是仍未产生较好效果。传统方式仍无法自动适应攻击者的逃逸绕过，策略升级也经常需要长达数月时间，存在严重的滞后效应，对未知攻击甚至完全无法察觉。可见，传统安全倚重旧范式，基于特征、规则和人工分析，存在安全可见性盲区，有严重的滞后效应、无力检测未知攻击、容易被绕过，以及难以适应攻防对抗的网络现实和快速变化的企业环境、外部威胁等问题。



图 2 安全转向数据科学驱动的新范式

如图 2 所示，通过对困境的持续探索，安全行业逐渐转向基于大数据驱动、安全分析和机器学习的安全新范式，以期弥补传统安全短板。同时，网络安全也已经开始从单纯强调边界防护到纵深安

全检测响应的艰巨转变。攻击者的不对称性优势，一直是安全团队面临的最大问题。只要能充分利用行为分析这块拼图，以及充分利用网络纵深路径上的各种数据，安全团队可能逆转这种不对称的情况，从海量的安全数据中识别和发现攻击和恶意行为 。

用户实体行为分析（UEBA）就是安全新范式的一个典型体现，其新范式的破局之道主要体现在如下五个方面：

1.行为分析导向

身份权限可能被窃取，但是行为模式难以模仿。内部威胁、外部攻击难以在基于行为的分析中完全隐藏、绕过或逃逸，行为异常成为首要的威胁信号。采集充分的数据和适当的分析，可发现横向移动、数据传输、持续回连等异常行为。

2.聚焦用户与实体

一切的威胁都来源于人，一切的攻击最终都会必然落在帐号、机器、数据资产和应用程序等实体上。通过持续跟踪用户和实体的行为，持续进行风险评估，可以使安全团队最全面地了解内部威胁风险，将日志、告警、事件、异常与用户和实体关联，构建完整的时间线。通过聚焦用户与实体，安全团队可以摆脱告警疲惫，聚焦到业务最关注的风险、有的放矢，提升安全运营绩效，同时通过聚焦到以账号、资产和关键数据为中心，可以大幅降低误报告警数量。

3.全时空分析

行为分析不再是孤立的针对每个独立事件，而是采用全时空分析方法，连接起过去（历史基线）、现在（正在发生的事件）、未来（预测的趋势），也连接起个体、群组、部门、相似职能的行为模式。通过结合丰富的上下文，安全团队可以从多源异构数据中以多视角、多维度对用户和实体的行为进行全方位分析，发现异常。

4. 机器学习驱动

行为分析大量的采用统计分析、时序分析等基本数据分析技术，以及非监督学习、有监督学习、深度学习等高级分析技术。通过机器学习技术，可以从行为数据中捕捉人类无法感知、无法认知的细微之处，找到潜藏在表象之下异常之处。同时机器学习驱动的行为分析，避免了人工设置阈值的困难和无效。

5. 异常检测

行为分析的目的，是发现异常，从正常用户中发现异常的恶意用户，从用户的正常行为中发现异常的恶意行为。

总结新范式破局的五个方面，就是在全时空的上下文中聚焦用户和实体，利用机器学习驱动方法对行为进行分析，从而发现异常。

（三）UEBA 的定义与演进

Gartner 对 UEBA 的定义是“UEBA 提供画像及基于各种分析方法的异常检测，通常是基本分析方法（利用签名的规则、模式匹配、简单统计、阈值等）和高级分析方法（监督和无监督的机器学习等），

用打包分析来评估用户和其他实体（主机、应用程序、网络、数据库等），发现与用户或实体标准画像或行为相异常的活动所相关的潜在事件。这些活动包括受信内部或第三方人员对系统的异常访问（用户异常），或外部攻击者绕过安全控制措施的入侵（异常用户）”[14]。

Gartner 认为 UEBA 是可以改变游戏规则的一种预测性工具，其特点是将注意力集中在最高风险的领域，从而让安全团队可以主动管理网络信息安全。UEBA 可以识别历来无法基于日志或网络的解决方案识别的异常，是对安全信息与事件管理（SIEM）的有效补充。虽然经过多年的验证，SIEM 已成为行业中一种有价值的必要技术，但是 SIEM 尚未具备帐户级可见性，因此安全团队无法根据需要快速检测、响应和控制[15]。

作为现代化 SIEM 演进的方向，如图 3 所示，SIEM、UEBA、安全编排自动化响应（SOAR）将会走向融合。

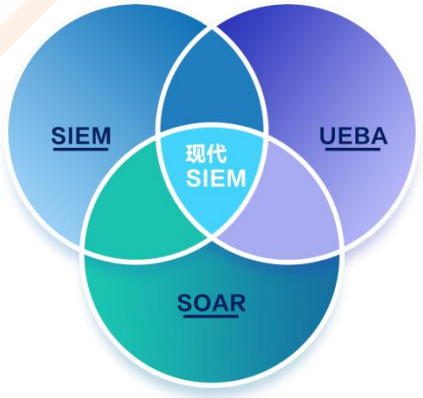


图 3 SIEM、UEBA、SOAR 的融合趋势

[14] 2019 Market Guide for User and Entity Behavior Analytics，Gartner，2019
[15] 2019 Market Guide for User and Entity Behavior Analytics，Gartner，2019

如图 4 展示 UEBA 的发展历程。由于身份和访问管理（IAM）无法提供全面的数据分析等原因，UEBA 的前身用户行为分析（UBA）应运而生。随后，来自于用户侧强劲的需求不断推动 UEBA 市场持续快速增长，复合年增长率达到了 48%。

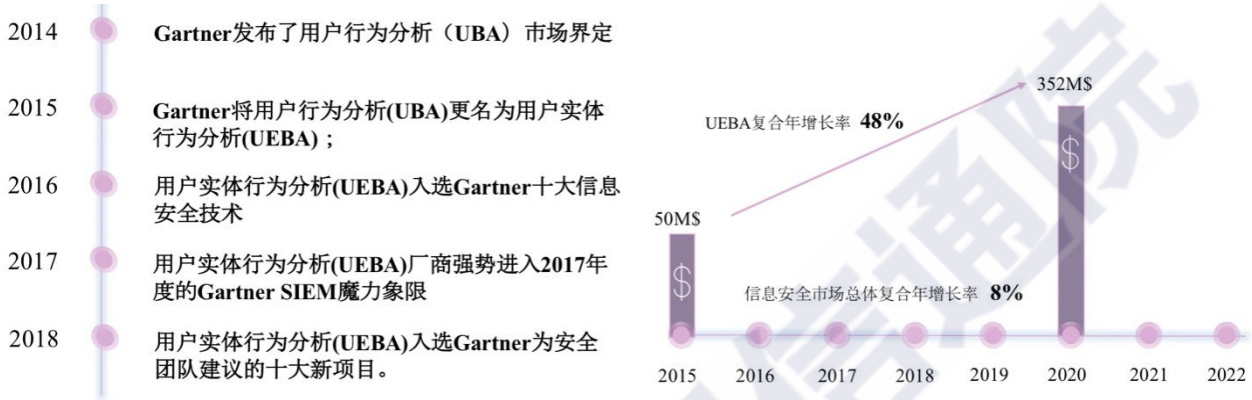


图 4 UEBA 的发展现状

如表 1 所示，市场上参与 UEBA 的厂商也逐渐增多，从早期独立的纯 UEBA 厂商，到主流 SIEM 厂商、网络流量分析（NTA）厂商也开始引入 UEBA 能力特性。

表 1 海外市场上的主流 UEBA 厂商分类

独立的纯UEBA		作为SIEM特性的UEBA		作为NTA特性的UEBA	
厂商	产品	厂商	产品	厂商	产品
Aruba	Introspect	Exabeam	Advanced Analytics	Cisco	UEBA
Bay Dynamics	Risk Fabric	FireEye	Helix	Darktrace	UEBA
Exabeam	Advanced Analytics	IBM	Qradar	Awake Security	Awake Security Platform
Force Point	UEBA	LogRhythm	UserXDR	ExtraHop	Reveal(x)
Gurucul	UEBA	McAfee	UEBA	Fidelis Cybersecurity	Elevate
Micro Focus	Interset	Micro Focus	Interset	FireEye	Helix
Securonix	UEBA	Microsoft	Advanced Threat Analytics	Aruba	Introspect
LogRhythm	UEBA	Rapid7	InsightIDR	Lastline	Analyst
Splunk	UEBA	Securonix	UEBA	Plixer	UEBA
DELL Technologies(RSA)	NetWitness UEBA	DELL Technologies(RSA)	UEBA	Vectra	Cognito platform
		Splunk	User Behavior Analytics		

（四）UEBA 的价值

通过对比安全新旧范式，可以看到 UEBA 具有明显的独特价值。UEBA 可以给安全团队带来独特的视角和能力，即通过行为层面的数据源以及各种高级分析，增强现有安全工具能力，提高风险可视性，弥补了安全运营中长久以来缺失的、极度有价值的视角，并提高了现有安全工具的投资回报率。

UEBA 比现有的分散工具具有更大的风险可视性，尤其是经过评分排序的威胁线索减少了噪音和误报告警。通过直观的点击式界面访问上下文和原始事件，从而加速了事件调查和根本原因分析，缩短了调查时间，降低了事件调查人数以及与雇用外部顾问相关的成本。

在增加现有安全投资的回报方面,UEBA 主要通过以下方式实现：安全信息和事件管理（SIEM）系统、恶意软件威胁检测工具端点检

测响应（EDR）和端点平台保护（EPP），以及数据泄漏防护（DLP）技术自动确定威胁和风险的优先级。通过无监督的机器学习来自动化、大规模的正常和异常行为的统计测量，从而降低了运营成本，实现无需管理复杂的基于阈值、规则或策略的环境。

表 2 各种安全技术和范式对比

	UEBA/行为分析	IDS/AV/WAF	TI/威胁情报
适用数据源	★★★★	★★★★	★★
可应用场景	★★★★	★★★★	★★★
攻防对抗	★★★★★	★★	★★★★
无滞后效应	★★★★★	★★	★★★
未知攻击	★★★★★	★	★★
环境自适应	★★★★★	★★★	★★★

如表 2 所示，UEBA 的价值主要体现在：

1. 发现未知

UEBA 可以帮助安全团队发现网络中隐藏的、或未知威胁，包括外部攻击和内部威胁；可以自适应动态的环境变化和业务变化；通过异常评分的定量分析，分析全部事件，无需硬编码的阈值，即使表面看起来细微的、慢速的、潜伏的行为，也可能被检测出来。

2. 增强安全可见

UEBA 可以监控所有账号，无论是特权管理员、内部员工、供应商员工、合作伙伴等；利用行为路径分析，贯穿从边界到核心资产

的全流程，扩展了对关键数据等资产的保护；对用户离线、机器移动到公司网络外等情况，均增强了保护；准确检测横向移动行为，无论来自内部还是外部，都可能可以在敏感数据泄露之前发现端倪，从而阻止损害发生；可以降低威胁检测和数据保护计划的总体成本和复杂性，同时显著降低风险以及对组织产生的实际威胁。

3.提升能效

UEBA 无需设定阈值，让安全团队更有效率。引入全时空上下文，结合历史基线和群组对比，将告警呈现在完整的全时空上下文中，无需安全团队浪费时间手动关联，降低验证、调查、响应的时间；当攻击发生时，分析引擎可以连接起事件、实体、异常等，安全人员可以看清全貌，快速进行验证和事故响应；促使安全团队聚焦在真实风险和确切威胁，提升威胁检测的效率。

4.降低成本

UEBA 通过聚合异常，相比 SIEM、DLP 等工具，大量降低总体告警量和误报告警量，从而降低安全运营工作负载，提升投资回报率（ROI）；通过缩短检测时间、增加准确性，降低安全管理成本和复杂性，降低安全运营成本；无监督、半监督机器学习让安全分析可以自动化构建行为基线，无需复杂的阈值设置、规则策略定制，缓解人员短缺问题；通过追踪溯源及取证，简化事故调查和根因分析，缩短调查时间，降低每事故耗费的调查工时，以及外部咨询开销；

通过自动化进行威胁及风险排序定级，提升已有安全投资(包括SIEM、EDR、DLP 等)的价值回报。

总之，UEBA 的价值主要体现在发现未知、增强安全可见、提升能效、降低成本。

CAICT 中国信通院

二、架构与技术

UEBA 是一个完整的系统，涉及到算法、工程等检测部分，以及用户实体风险评分排序、调查等用户交互、反馈。从架构上来看，UEBA 系统包含三个层次，分别是数据中心层、算法分析层、场景应用层。其中，算法分析层一般运行在实时流处理、近线增量处理、离线批量处理的大数据计算平台之上。典型的完整 UEBA 架构如图 5 所示。



图 5 典型的 UEBA 系统架构

该平台运行着传统的规则引擎、关联引擎，同时也支持人工智能引擎，如基线及群组分析、异常检测、集成学习风险评分、安全知识图谱、强化学习等 UEBA 核心技术。

（一）基线及群组分析

以史为鉴，可以知兴替。历史基线，是行为分析的重要部分，可以进行异常检测、风险评分等。以人为鉴，可以明得失。通过构

建群组分析，可以跨越单个用户、实体的局限，看到更大的事实；通过对比群组，易于异常检测；通过概率评估可以降低误报，提升信噪比；组合基线分析、群组分析，可以构成全时空的上下文环境。如图 6 所示，展现了几个人员的历史基线以及群组分析。

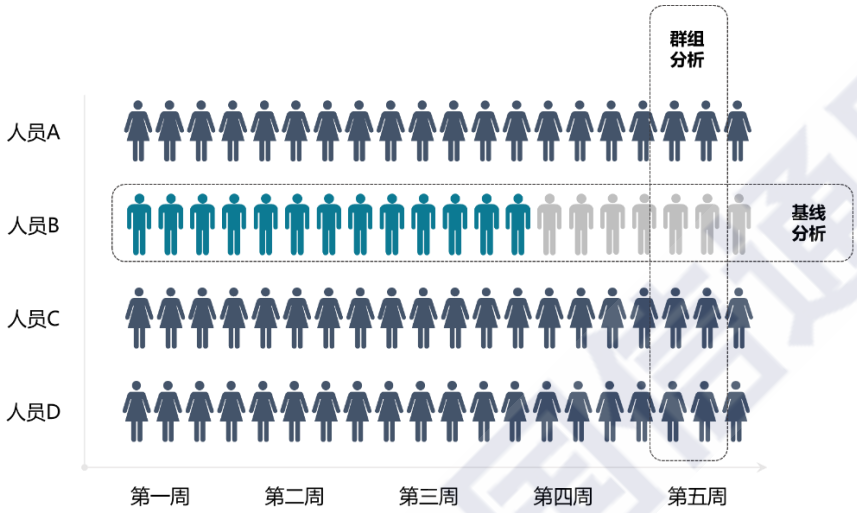


图 6 基线分析与群组分析

（二）异常检测

异常检测关注发现统计指标异常、时序异常、序列异常、模式异常等异常信号，采用的技术包括孤立森林、K 均值聚类、时序分析、异常检测、变点检测等传统机器学习算法。其中，基于孤立森林的异常检测效果图如图 7 所示。现代的异常检测也利用深度学习技术，包括基于变分自编码器（VAE）的深度表征重建异常检测、基于循环神经网络（RNN）和长短时记忆网络（LSTM）的序列深度网络异常检测、图神经网络（GNN）的模式异常检测等。针对标记数据缺乏的现状，某些 UEBA 系统能够采用主动学习技术（Active Learning）、自学习（Self Learning），充分发掘标记数据和无标记数据的价值。

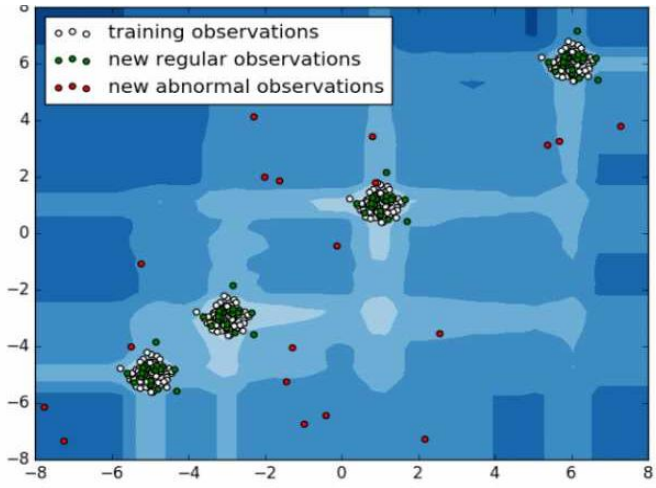


图 7 孤立森林发现异常点

（三）集成学习风险评分

UEBA 作为一种新范式，把安全运维从事件管理转换到用户、实体风险，极大的降低工作量、提升效率。其中，实现转换的关键在于使用集成学习进行风险评分。如图 8 所示，风险评分需要综合各种告警、异常，以及进行群组对比分析和历史趋势。同时，风险评分技术中用户间风险的传导同样重要，需要一套类似谷歌搜索使用的网页排名 PageRank 算法的迭代评估机制。风险评分的好坏，将直接影响到 UEBA 实施的成效，进而直接影响到安全运营的效率。

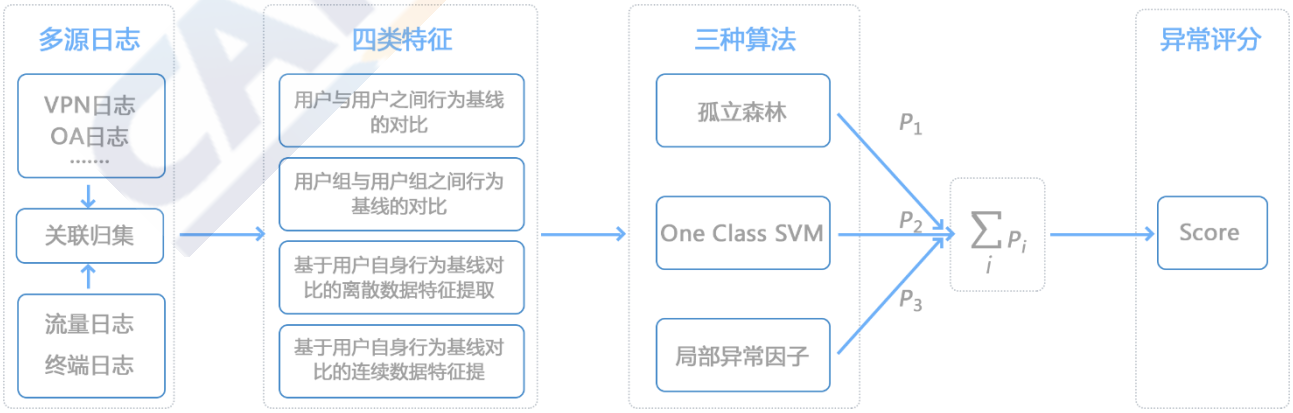


图 8 多种算法进行集成学习

（四）安全知识图谱

知识图谱已经成为人工智能领域的热点方向，在网络安全中同样也有巨大的应用潜力。部分 UEBA 系统已经支持一定的安全知识图谱能力，可以将从事件、告警、异常、访问中抽取出的实体及实体间关系，构建成一张网络图谱，如图 9 所示。任何一个事件、告警、异常，都可以集成到网络图谱中，直观、明晰的呈现多层关系，可以让分析抵达更远的边界，触达更隐蔽的联系，揭露出最细微的线索。结合攻击链和知识图谱的关系回放，还能够让安全分析师近似真实的复现攻击全过程，了解攻击的路径与脆弱点，评估潜在的受影响资产，从而更好的进行应急响应与处置。

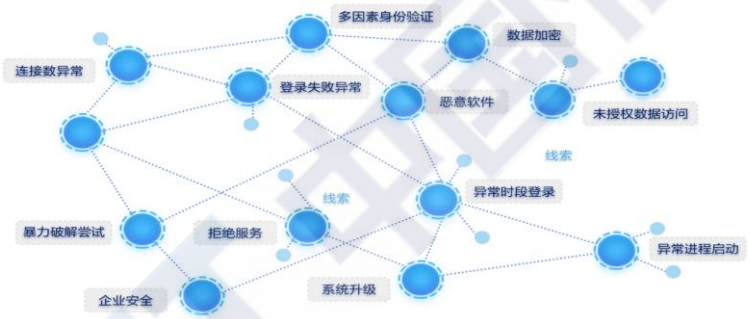


图 9 安全知识图谱

（五）强化学习

不同客户的环境数据源的多元性及差异性，以及用户对异常风险的定义各有不同， UEBA 需要具有一定的自适应性，“入乡随俗”输出更精准的异常风险。强化学习能够根据排查结果自适应地调整正负权重反馈给系统，进而得到更符合客户期望的风险评分。如图 10 所示，UEBA 给出异常信号后，结合安全管理人员的排查结果，获

取反馈奖赏或惩罚，通过学习进行正负权重调整，从而让整体效果持续优化改进。

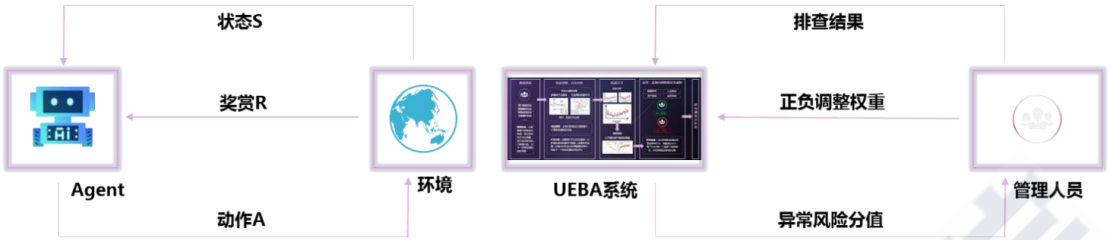


图 10　UEBA 中的强化学习

（六）其他技术

除了以上 5 个主要关键技术外,UEBA 一般还使用到了特征工程、会话重组、身份识别。

1. 特征工程

如何从行为模式中提取合理特征向量？有些特征在不同业务系统之间通用，有些特征需要根据业务场景具体分析，涉及到如何合理、高效设计指标体系，一般需要参考 5W1H 模型（又称六何法，或 6W 分析法，即何人（Who）、何事（What）、何时（When）、何地（Where）、何解（Why）及如何（How）。由这六个疑问词所组成的问句，均不是是非题，而是需要一个或多个事实佐证的应用题）。

2. 会话重组

会话对象为每个用户从会话启动到终止缝合所有事件，并将这些事件与用户联系起来，即使更改了帐户、更改了设备或更改了 IP。通过查找启动会话的事件，如 Kerberos 或 NTLM 登录、VPN 事件、应

用程序登录、物理打卡记录等，开启生成会话；登出、打卡离开、超时或其他信号指示会话结束。会话的风险得分是分配给会话中每个活动的风险分数的总和。

3. 身份识别

在识别同一个用户、实体过程中，并不是所有环境中都有集中认知管理，同一个用户、实体，在不同的系统中的标识、用户名可能不同，需要把这些行为关联到同一个身份标示上，才能让行为画像、异常检测更准确更有效。

CAICT 中国信通院

三、部署实施

（一）聚焦目标

UEBA 部署实施的目标有很多，例如：组织当前最大的安全焦虑是什么？管理层对于企业安全的最大担忧是什么？组织所处行业的安全环境如何？最大的安全威胁是什么，是用户隐私数据保护，还是内部安全威胁？安全团队的使命是什么？安全运营的关键绩效指标是什么？

安全负责人和安全团队需要认真深入的思考上述问题，并和各利益相关者紧密沟通，提出自身视角的安全关切。组织的安全不仅仅是首席信息安全官（CISO）和安全团队的职责，需要最高管理层的反馈和资源保障，同时需要把安全放到数字经济、业务连续性的视角进行全面评估。

（二）识别数据源与接入数据

从部署规划角度，UEBA 接入的数据源主要包括主机、终端、网络设备、安全设备、业务系统、应用系统、物理安全系统等。接入的数据格式主要包括日志、网络流量两大类，以及组织内各种上下文数据。

具体来说，为了有效的评估检测用户及实体的行为，可以根据情况选择，应该包括但不限于虚拟私人网络（VPN）日志、高级可持续威胁防御系统（APT）日志、入侵防御系统（IPS）日志、入侵检

测系统（IDS）日志、WEB 应用防护系统（WAF）日志、网络流量分析系统（NTA）日志、深度报文解析系统（DPI）日志、Windows 主机日志、Linux 主机日志、Unix 主机日志、邮件审计（Mail Audit）日志、终端检测与响应系统（EDR）日志、应用程序接口服务（API 服务）访问日志、上网行为审计（SWG）日志、数据库审计日志、统一运维管理平台（USM）日志、堡垒机日志、微软系统监控（SYSMON）日志、网络防火墙（FW 和 NGFW）日志等数据。

此外，比较有价值的数据源还包括物理安全系统，如门禁打卡日志、饭卡消费日志、车库出入日志、监控日志、钉钉考勤记录等。

同时建议接入如威胁情报数据、活动目录域（AD）日志、身份访问管理（IAM）数据、配置变更管理（CMDB）记录、人力资源系统（HR）记录、办公自动化系统（OA）记录等。

（三）确定部署模式

在评估 UEBA 方案时，首先需要根据组织的信息系统架构、业务数据流、数据量进行审慎评估，比如部分厂商仅提供客户本地部署，部分厂商同时还支持云化（比如虚拟化及容器化）部署，以及软件即服务（SAAS）化部署。UEBA 系统部署位置和数据源的位置，直接影响到 UEBA 数据集成的速度，对网络延时的容忍度较低，数据传输的带宽成本同样也是一个重要的考虑因素。

（四）分析微调与定制

主流的 UEBA 系统会提供一定数量的内置分析模型（Pre-Packaged Analytics），开箱即用，可以较好自适应常用环境和典型场景。部署完成后，一般情况下通过 2 到 4 周的时间学习构建基线，即可开始有效运作。

但是每个组织都有自己的业务特征，采用的信息技术存在差异，行为数据存在一些细微甚至较大的差异，需要进行一些微调，比如增加一些特征或调整权重。可以根据业务领域知识，多尝试一些可能有效的特征、算法，通过持续的权重微调，让重要有效的凸显出来。

（五）迭代优化

与 SIEM 实施类似，UEBA 实施也是一个迭代优化、持续改进的过程，是数据科学在安全领域的应用，需要遵循 PDCA 循环。UEBA 还需要持续的探索不同的数据源、不同的数据特征、不同的检测算法，以更好的提升异常检测性能，改进威胁检测响应的能力和效率。

如图 11 所示，根据新业务场景的需求分析，可能需要接入新数据 、探索新特征工程、测试新算法、进行反馈调优，以便满足项目的安全分析检测需求。



图 11 UEBA 分析改进与迭代调优循环流程

四、最佳实践

（一）专职团队

专注于协调和部署的项目团队，是成功的基础。安全运营首要因素始终是人，建议 UEBA 实施需要有专职团队负责，确保团队人员拥有专业技能和素养，熟悉安全攻防，拥有数据分析、机器学习算法等知识，最好能组建多种技能配合协调的多样性团队。

（二）专注于用例开发

Gartner 客户报告显示,需要花三到六个月的时间才能完整启动 UEBA 计划，调整和交付部署的用例，并从一小部分定义良好的用例和一组有限的数据开始，为更长的项目时间表做好准备。[16]

安全团队应该基于组织所属行业特点、业务风险视角，专注于用例开发，建议重点关注如特权账号行为、少见及可疑的网络活动、异常的访问模式、异常的通信流量、隧道传输等。

由于 UEBA 的典型用例部署生效需要 2 至 4 周不等，分析案例应该保持持续的迭代改进。

（三）法律合规性

一方面，UEBA 项目的规划、立项、测试、运营过程，需要法务部门的支持与协助。数据源的采集与分析处理过程，应确保合规。为确保数据收集、分析的法律合规性，在项目实施前期，法务部门

[16] 2019 Market Guide for User and Entity Behavior Analytics，Gartner，2019

应当介入，明确数据收集范围、数据属性、数据留存周期，确保数据分析过程都符合相关法律和监管规则，并正确反映到用户协议、使用条款、雇员保密协议等法律文件中。

另一方面，应做好细粒度的访问控制，进行合适的网络隔离，控制数据传播范围，进行全面的内部操作审计，保持持续监控，防止数据泄漏、权限滥用。

CAICT 中国信通院

五、典型应用案例

（一）恶意内部人员

根据 Haystax 于 2019 年发布的网络内部安全威胁报告，如图 12 所示，内部威胁是造成数据泄露的第二大原因。往往因为非授权访问、雇员和外包员工工作失误等原因，导致“合法用户”可以非法访问特定的业务和数据资源，造成组织内部数据泄漏。[17]从本质上讲，恶意内部威胁来自具有试图对雇主施加损害等恶意意图的可信用户。由于难以评估恶意意图，需要分析数据中难以获取的上下文行为信息。

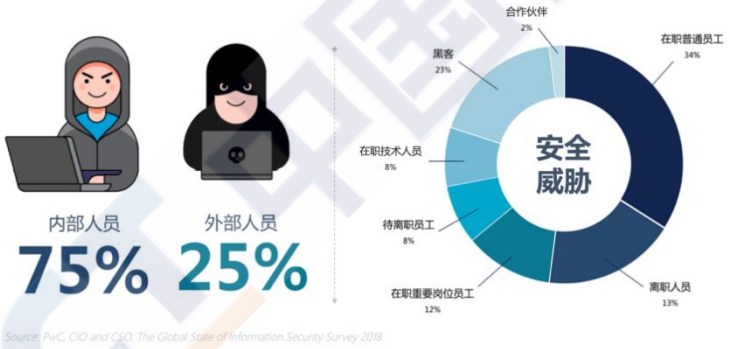


图 12 内部人员导致的安全威胁

内部人员窃取敏感数据是企业典型的内部威胁场景。由于内部人员具备企业数据资产的合法访问权限，且通常了解企业敏感数据的存放位置，因此通过传统的行为审计手段无法检测该类行为。但是利用 UEBA 技术，选取敏感数据访问相关的特征，构建企业员工和系统创建正常的活动基线、用户画像，可以通过基线构建模型用于判断是否存在内部人员窃取敏感数据行为。

[17] 2019 INSIDER THREAT REPORT，Haystax，2019

针对此类场景，UEBA 解决方案通过治理组织的数据库日志、回话日志、用户访问日志以及访问全流量等信息，生成敏感数据访问周期、时序、动作、频繁度等相关特征，通过时序关联和自学习算法生成敏感数据被访问的动态基线、用户访问动态基线、群体访问动态基线。

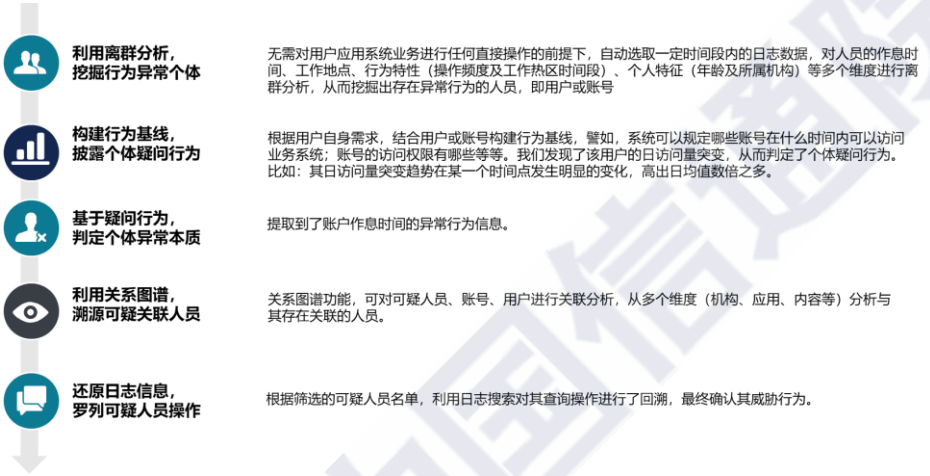


图 13 内部员工窃取敏感数据场景分析流程图

利用动态基线，通过如图 13 所示流程，可实现对高频、越权、伪造身份、冒用身份、数据窃取等多种异常行为的分析和检测，进一步关联敏感数据的访问特征，定位是否存在内部人员窃取敏感数据行为，保障企业核心数据资产的安全。

（二）失陷账号

账号盗用一直是困扰各种组织的痛点，且涉及到最终用户的利益和体验，特权账号更是黑客瞄准的攻击目标。如图 14 所示，攻击者一旦渗透进组织边界且获取失陷账号后，会在组织内部网络中横向移动，形成高级持续性威胁（APT）以及未知或尚无法理解的各种威胁，比如众所周知的零日攻击，该类攻击行为难以发现，并且通常隐藏在合法用户或服务帐户的面纱之下。



图 14 账号失陷是攻击链模型中的转折点

传统范式难以对付该类攻击，同时难以跟随攻击者的技术升级。该类威胁通常有一个复杂的作战模式如攻击链，而且会长期留存，其中大部分行为尚未被认定为恶意行为，通过简单的分析如模式匹配、阈值或关联规则均难以检测。

然而，许多高级威胁会使得用户和资产行为方式与平时不同，如失陷账号。针对此类场景，UEBA 通过对正常行为和人员进行抽象归纳，利用大数据技术生成个体行为画像和群体行为画像。在此基础上，对比账户的活动是否存在异常行为，如频繁登录和退出、访

问历史未访问过的信息系统或数据资产、异常时间地点登录等，并对比分析账户的活动是否偏离个人行为画像和群体（如部门或项目组等）行为画像，综合判断账户疑似被盗用风险评分，帮助安全团队及时发现账号失陷。

UEBA 技术为检测失陷账号提供了最佳的安全视角，提高了数据的信噪比，可合并和减少告警量，让安全团队优先处理正在进行的威胁，并且促进有效的响应调查。

同时，UEBA 还可针对已建立的账号监视分析用户行为，识别过多的特权或异常访问权限，适用于特权用户和服务帐户等所有类型的用户和帐户。使用 UEBA 还可以用来帮助清理帐户和权限设置高于所需权限的休眠帐户和用户权限。通过 UEBA 的行为分析，身份识别与访问管理（IAM）和特权账号管理（PAM）系统能够更全面的进行访问主体安全性评估，支持零信任（Zero Trust）网络安全架构和部署场景。动态权限策略控制是零信任的核心能力，而 UEBA 已经成为实现动态权限策略控制最有效的方法。

（三）失陷主机

失陷主机是典型的企业内部威胁之一，如图 15 所示，攻击者常常通过入侵内网服务器，形成“肉机”后对企业网络进行横向攻击。基于此类场景的特性分析，失陷主机通常包含回链宿主机和内网横向扩散两大重要特征。



图 15 主机失陷是病毒爆发、勒索软件的前奏

针对此类场景，UEBA 可构建时序异常检测模型，根据企业内网主机或服务器时序特征的历史时序波动规律，以及请求域名、账户登录、流量大小、访问安全区频繁度、链接主机标准差等特征，构建单服务器的动态行为基线，群体（如业务类型、安全域等）服务器动态行为基线。

利用基线，考虑具体的主机疑似失陷场景，如僵尸网络、勒索病毒、命令控制（C&C 或 C2）等，给出不同模型不同实体在不同时间段的综合异常评分，从而检测失陷主机，并结合资产信息，定位到具体的时间段和主机信息，辅助企业及时发现失陷主机并溯源处理。

（四）数据泄露

数据泄露可能给组织的品牌声誉带来严重损失，导致巨大的公关压力，是组织最关注的安全威胁之一。内部员工窃取敏感数据是企业典型的数据泄漏场景，由于内部员工具备企业数据资产的合法

访问权限，且通常了解企业敏感数据的存放位置，因此通过传统的行为审计手段无法有效检测该类行为。

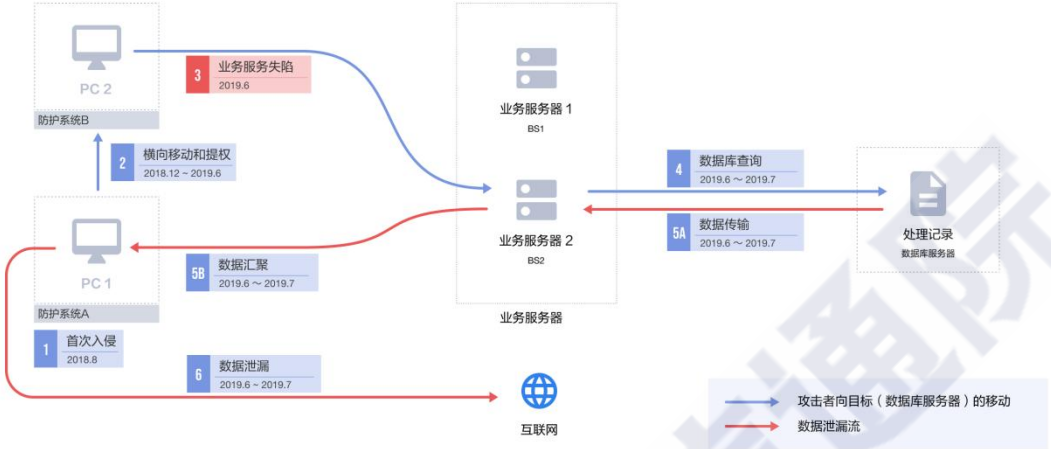


图 16 数据泄漏中的攻击移动和数据流

UEBA 可以增强 DLP 系统，使其具有异常检测和高级行为分析功能。通过对数据访问行为的分析，结合其他上下文，融入网络流量（如 Web 安全代理）和端点数据进行分析，有助于了解数据传输活动。组合 UEBA 和 DLP，数据泄露检测可以用于捕获内部人员和外部黑客组织。

如图 16 所示，根据数据泄漏的技术、方法及途径，选取敏感数据访问相关的特征，构建企业员工和系统创建正常的活动基线和用户画像，判断是否存在内部员工窃取敏感数据行为。针对此类场景，UEBA 解决方案通过治理企业数据库日志、回话日志、用户访问日志以及访问全流量等信息，生成敏感数据访问相关特征，如访问周期、时序、动作、频繁度等，通过时序关联和自学习算法生成敏感数据

库的被访问动态基线、用户访问动态基线、群体访问动态基线等多种检测场景。

（五）风险定级排序

由于安全团队人力资源有限，所有组织几乎都面临告警过量的问题，难以全面处理各个安全设备触发的安全告警。根据 SANS 2019 事故响应调查报告，57%的受访者认为安全团队人员短缺和技能短缺是主要障碍。[18] 如何让有限宝贵的人力资源投入，带来最大的安全运营收益，成为风险排序定级的价值所在。

UEBA 不仅使用基线和威胁模型，而且也会根据所有安全解决方案中生成的报警，构建用户及实体的行为时间线，进行风险聚合。通常也会结合组织结构、资产关键性、人员角色和访问级别等进行权重评估，进行综合风险定级并排序，从而明确用户、实体、事件或潜在事件应该优先处理范围。通过风险定级排序，可以极大的缓解安全团队人力短缺的现状。

为了构建现代化 SIEM（Modern SIEM）能力，安全团队可以将 SIEM、UEBA、安全编排自动化响应（SOAR）结合，进行数据双向集成，透过 SOAR 的安全编排，进行安全告警的分析和分类，利用人机结合的方式对安全事件进行定义、划分优先级，建立标准化安全事

[18] Incident Response (IR) Survey: It’s Time for a Change，SANS Institute，2019

件的处理工作流，从而达到一体化安全运营，提升安全团队整体协同，形成行为异常的检测与响应闭环。[19]

比如在某市医疗机构出现勒索病毒事件后，安全团队需要进行应急响应，可是应该从何处着手？等待数据被加密收到勒索通知后，再处理就为时已晚。如果该机构部署了 UEBA，就可以快速分析文件创建、文件读取、磁盘读取、磁盘写入等行为，发现可疑的病毒感染资产，基于风险进行定级排序，对高风险资产优先进行隔离处理。安全团队还可以进行回溯调查，明确勒索病毒的传染源、传播扩散的路径，有针对性的进行网络阻断，遏制勒索病毒的进一步爆发。

另一方面，如果该机构一直持续监控这些勒索病毒相关的行为特征，持续检测异常行为，就可能在勒索发生前及时阻止事件的发生。

（六）业务 API 安全

企业 WEB 业务系统通常会提供大量的业务应用编程接口（API），如登录 API、数据获取 API、业务调用 API 等，攻击者通过对具体网站访问数据或请求数据进行抓包，可获取企业业务 API 入口的大致范围，通过对这些 API 进行恶意调用，可实现恶意访问、数据窃取以及其他相关恶意活动，严重影响企业的正常业务开展。

针对此类场景，攻击者可能利用变换多个不同的请求参数已达到恶意调用 API 的目的。UEBA 通过分析目前常用的 API 组成和使用

[19] 网络安全先进技术与应用发展系列白皮书安全编排自动化响应，中国信息通信研究院，2018

方式，通常包括 API 所对应的 URL 请求参数和请求主体两部分，通过提取企业业务 API 访问频率特征、请求者访问频率特征、参数变换标准差、以及请求时间昼夜分布等特征，构建 API 请求频率动态基线、API 请求时序动态基线、参数变换动态基线等多种检测场景。

基于动态基线，实现检测对 API 请求量突变异常检、周期性异常、未知用户、可疑群体潜伏用户（某用户使用大量不同 IP）等异常行为，进一步结合 API 的具体业务属性，实现 WEB 业务系统 API 异常请求行为检测，可定位到具体的时间段和业务、数据信息，辅助企业及时发现异常调用行为，保证整体业务和数据安全。

（七）远程办公安全

远程办公可以解决疫情等特殊时期的企业复工需要，但是同时也会带来一些额外的网络安全风险，促使基于用户行为分析新范式发挥其价值所在。

企业一般通过 VPN 进行远程办公，从而隔离避免外部人员直接能访问到内部资源，同时也会带来一定的安全风险。

UEBA 可以收集 VPN 及内部流量日志，构建涵盖每个员工登录地点、登录时间、在线时长、网络行为、协议分布等特征的行为画像。通过对比用户的历史行为基线，以及对比同组人员的行为基线，可以第一时间发现可疑的人员账号，通过调查分析，及时防范 VPN 账号违规操作或账号失陷风险。

六、行业应用案例

（一）医疗行业

随着医院信息化的迅猛发展，信息的高度集中使得核心数据泄密的隐患也越来越突出，在利益的驱使下非法统方行为时有发生，严重影响了医院的公众形象，也严重损害了患者的利益。鉴于问题严重性，引起了管理部门的高度重视，尽管多数医院也采取了“教育为先、制度为主”的管理手段，但仍难以达到预期效果。

目前医院主要面临的问题是：

1、核心数据维护人员越来越多，既有本院相关业务科室信息维护人员，也有系统开发商、第三方运维外包公司；

2、非法统方手段专业化，由早期的手工统方转变成专业的统方软件，只需要在医院任何一台电脑上运行程序，就可以非常快捷的完成统方；

针对此类场景，UEBA 通过动态建模即根据历史的数据库访问情况，建立一套系统数据库的用户访问行为模型，包括帐号、IP 地址、客户端工具、SQL 语句、返回结果等成千上万个动态元素，并根据数据库的变化情况持续更新。当有新的行为发生时系统通过高效的算法比对模型的各种参数，进而根据其与模型的偏离情况来智能识别统方行为。

（二）金融行业

手机银行、信用卡网申、网上信贷、快捷支付等银行线上便捷业务的流行给不法分子带来可乘之机。不法分子利用伪基站发送钓鱼链接，利用木马、社会工程或利用电信诈骗手段骗取和盗用用户账户信息和金融资产。黑客利用非法获得的储户信息进行撞库攻击，致使近年来在银行线上渠道发生了大量非本人交易等欺诈情况，给银行和储户都造成了严重的经济损失。

UEBA 在金融反欺诈方面具有独特优势。通过对银行储户各类渠道的历史登录和交易等行为的长周期数据特征提取，从历史行为数据中提取数量、关系、序列等信息，以此建立用户特征矩阵，运用机器学习技术建立每个储户的行为模型和行为基线。无论欺诈的手段和方式怎样变化，欺诈对象的行为模式一旦偏离历史基线，就会作为风险异常行为第一时间被发现。此外，UEBA 还可以运用针对银行的撞库攻击检测。基于银行各渠道的 IP 登录行为特征分析，以 IP 地址为核心，并量化多维度参数，运用机器学习算法对 IP 登录行为进行聚类分析，进而识别针对银行储户的撞库行为。

（三）能源行业

能源行业推出了充电移动端应用（App），其正常的使用流程如下：第一步：注册；第二步：登录找桩；第三步：插入充电卡，扫描 App，提枪充电。超过半数用户采取上述三步操作使用 App，同时也有部分用户进行非法操作。UEBA 通过收集来自终端的指纹位置信息、App 状态、App 登录、App 服务器等信息，并且关联充电量、充

电桩操作等信息，汇聚到服务端的分析引擎，构建各种特征，锁定行为异常的用户，可以及时发现并避免盗电、盗取敏感数据等安全风险。

（四）政务行业

随着“数字政府”的推进，政务数据正逐步走向集中管理并进行共享交换。如走在改革前列的杭州，提出了“最多跑一次”的口号，并成立大数据局推动政府数字化。数据汇总后，各部门进行查询调用，必然会带来数据异常访问、数据泄露以及数据勒索的数据安全问题。随着开源或商用数据库漏洞的不断爆发，MongoDB、CouchDB、ElasticSearch、Hadoop、Cassandra 以及 MySQL 等数据库逐渐成为数据勒索的目标。

数据勒索可能导致存储的数据被删除、被加密无法访问，对企业造成重大损失。此类场景通常存在撞库、遍历数据表、加密数据表字段、异常建表、异常删表等多种复杂操作行为。

针对此类场景，UEBA 通过分析数据库高危操作特征，如删表、删库、建表、更新、加密等行为，并通过用户活动行为提取用户行为特征，如登录、退出等，并在此基础上，构建登录检测动态基线、遍历行为动态基线、数据库操作行为动态基线等多种检测场景。

利用这些动态基线，可实现对撞库、遍历数据表、加密数据表字段、异常建表、异常删表以及潜伏性恶意行为等多种异常行为的分析和检测，将该类行为基于用户和实体关联，最终为用户输出恶

意用户和受影响的数据库，并提供影响数据库类型、行数、高危动作详情等溯源和取证信息，辅助安全团队及时发现问题并阻断攻击。

CAICT 中国信通院

七、总结

对于组织来说，提升网络安全能力需要深刻认识到渐变胜不变。简而言之，在安全方法方面，不能因为追求“完美”而错失“变好”的机会。和所有其他事物一样，没有百分百完美的安全方法。同时，并不存在能够解决所有网络安全挑战的“万全之策”。数字新时代面临的安全威胁形式复杂多变，攻击暴露面始终在不断变化和扩展，安全技术和战略也应相应的持续演进。

根据 Gartner 报告，UEBA 在中大型企业的一系列使用案例，已证明该技术已经成熟[20]。但是目前 UEBA 技术的应用仍然介于早期采用者和多数人阶段之间，UEBA 在相当长一段时间内仍将是一种可行且有用的技术，未来也将会成为主流，并且驱动越来越多的安全应用场景。

作为早期采用者，及时把握安全新范式，可以让组织获得快人一步的领先竞争优势，保障数字化转型更安全，为安全团队赋能，实现安全可见、可查、可控，促使安全运营提效降本。

[20] 2019 Market Guide for User and Entity Behavior Analytics，Gartner，2019

关于

中国信息通信研究院简介

中国信息通信研究院始建于 1957 年，是工业和信息化部直属科研事业单位。多年来，中国信通院始终秉持“国家高端专业智库 产业创新发展平台”的发展定位和“厚德实学 兴业致远”的核心文化价值理念，在行业发展的重大战略、规划、政策、标准和测试认证等方面发挥了有力支撑作用，为我国通信业跨越式发展和信息技术产业创新壮大起到了重要推动作用。

中国信息通信研究院安全研究所

中国信息通信研究院安全研究所，是专门从事 ICT 领域安全技术研究的科研机构，主要职责包括开展信息通信领域安全的战略性和、前瞻性、技术性问题研究，为国家主管部门有关网络安全发展战略、决策、规范的制定提供强有力的技术支撑。安全所拥有雄厚的网络安全技术评估评测能力以及高端的专业网络安全支撑团队，承担大量重大网络安全专项科研课题，牵头制定大量国际国内网络信息安全标准规范，对前沿新兴网络安全技术的研究有深厚积累。

杭州安恒信息技术股份有限公司

杭州安恒信息技术股份有限公司，是 2007 年 5 月由范渊先生创办的国家级高新技术企业，中国领先的信息安全产品和服务提供商。国内总部设在杭州及北京，并在上海、南京、广州、深圳、成都、武汉、重庆、济南、西安等三十多个城市设有分支机构，服务客户包括政府、公安、运营商、金融、教育、企业等多个行业。目前已是享誉国内外的网络安全品牌，于 2016 年成功跻身“全球网络安全 500 强中国区榜首”，并于 2019 年 11 月登陆科创板。

AiLPHA 大数据实验室

随着信息技术的飞速发展，传统安全设备无法解决越来越复杂和隐蔽的安全威胁。以安恒首席科学家刘博为核心的研发团队为此突破核心技术难点，安恒信息创建 AiLPHA 大数据实验室。实验室以“AI 驱动安全”为核心理念，研究超大规模存查、大数据实时智能分析、用户实体行为分析（UEBA）、多维态势安全视图、企业安全联动闭环等技术。目前具备全网流量处理、异构日志集成、核心数据安全分析、办公应用安全威胁挖掘等前沿大数据智能安全威胁挖掘分析与预警管控等核心能力。为企业用户提供全局态势感知和业务不间断稳定运行安全保障。致力于让安全更智能，更简单。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62308680

传真：010-62300264

网址：www.caict.ac.cn