X-Force

2021 IBM Security X-Force 内部威胁报告

IBM Security X-Force 威胁情报

特殊情报报告（2021 年第二季度）

IBM

目录

简介 03
主要研究成果 04

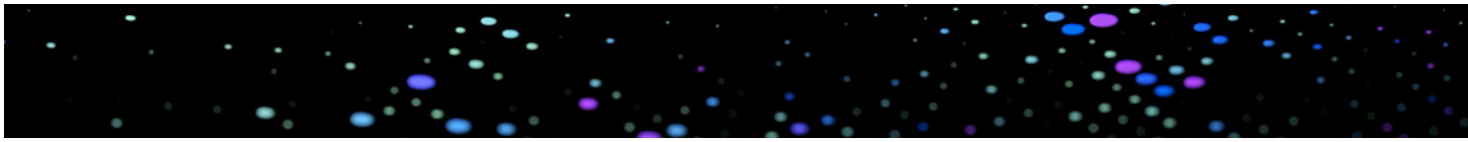
第一章
内部威胁攻击是如何被发现的 05

第二章
证据的缺乏以及 X-Force 调研中的未知因素 07

第三章
特权级访问权限与管理员访问权限 08

第四章
监督者由谁来监督? 09

第五章
建议 13



简介

网络威胁的形势正在不断发生变化，这是因为众多攻击者和防御者在新技术和新流程方面不断进行创新和突破。 2021 年，各大企业或机构的安全支出进一步增加了 10%，为保护资产并招募人才来防范和应对攻击，他们每年的花费总计高达 600 亿美元左右。[1]

企业或机构的安全重点和支出有很大一部分着眼于挫败外来攻击，而内部威胁却往往被忽视： 也就是那些来自企业内部的威胁。 我们知道，许多内部威胁属于非恶意的，或是意外发生的结果，但其有可能造成毁灭性的伤害，具体表现形式为数据盗窃、财务损失、知识产权盗窃和声誉损害。 Ponemon Institute 在 2020 年的一项调查中估计，为了从内部威胁事件中恢复（无论事件原因如何），各企业平均需要花费 644,852 美元。[2] 这其中包括了对可疑内部事件进行监测和调查，以及对内部事件进行响应、遏制、根除和补救所耗费的成本。

在本报告中，IBM Security X-Force 将相关内部人员定义为：

— 意外事件内部人员： 疏忽大意的员工或第三方供应商/承包商。[3]

— 恶意内部人员： 存在犯罪意图或恶意的员工或第三方供应商/承包商。

1. https://www.infosecurity-magazine.com/news/global-cybersecurity-spending-to/
2. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/
3. 疏忽大意的内部人员是指意外导致事件发生，从而影响了企业内部数据或系统的机密性、完整性或可用性的内部人员。 这其中不包括网络钓鱼/社会工程事件。

利用从实际的事件响应调查中收集的独家专有数据，X-Force 对 2018 至 2020 年间影响了各大企业或机构的可疑内部威胁事件（包括意外和恶意事件）进行了分析。对于诸多极其知名的内部威胁攻击问题，已有许多开源报道，而本报告将结合这些情况，就其中数据暴露出的重要发现依次进行深度分析：

— 大多数内部攻击是如何被发现的。

— 访问权限在内部攻击中发挥的作用。

— 缓解内部威胁的最佳实践操作。

主要研究成果

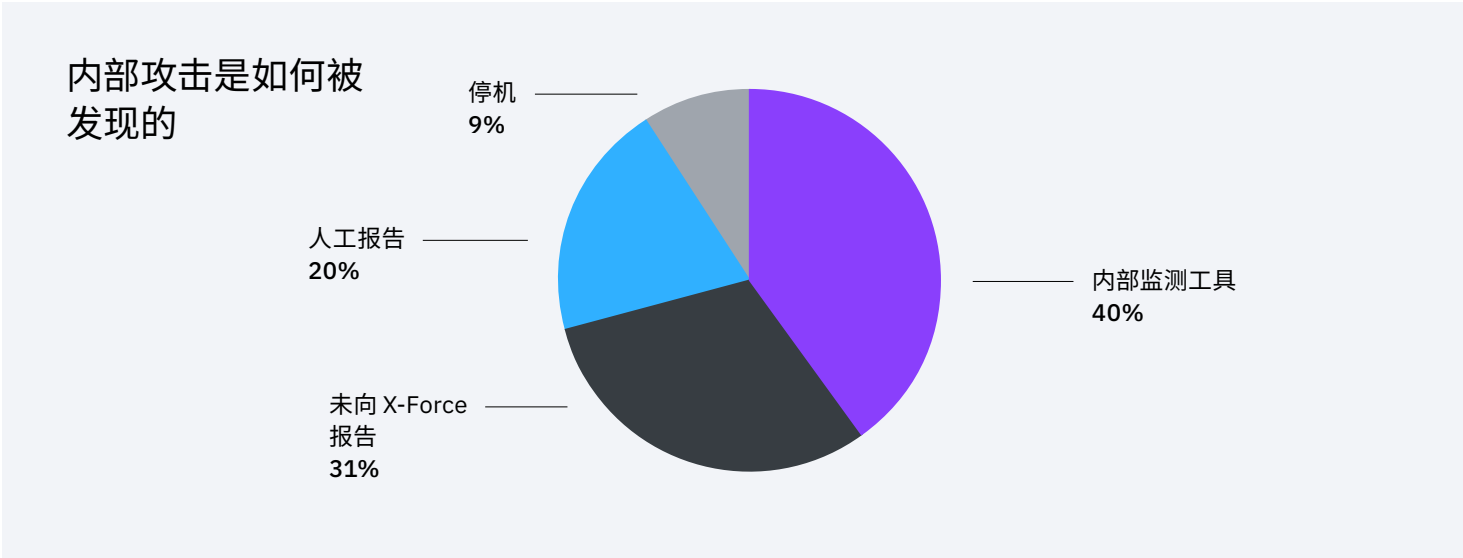
40% 的事件是通过内部监测工具生成的警报检测到的。

40% 的事件会涉及某位对公司资产拥有特权级访问权限的员工。

在 100% 的事件中，相关内部人员确实或可能拥有管理员访问权限，这种高级别访问权限会加剧事件本身的发展。

内部威胁攻击是如何被发现的

内部威胁通常是指对企业资产拥有一定访问权限的合法用户，因恶意或意外地利用了该访问权限而最终对企业造成伤害的攻击事件。 这种威胁可能来自现任或前任员工，也可能来自第三方承包商或供应商，他们拥有为所承担的业务职能提供服务所需的权限。



针对 X-Force 自 2018 年以来应对过的内部威胁予以分析后发现，此类事件有 40% 是通过内部监测工具生成的警报检测到的。人工报告（比如员工向其企业发出异常活动警报）的检测贡献值为 20%，另有 9% 的事件是因出现系统中断情况，安全团队收到了警报。

Ponemon Institute 在“内部威胁在2020 年制造的代价: 全球报告”(报告赞助方:ObserveIT 和 IBM)一文中指出，用户行为分析(UBA)、特权级访问管理(PAM)、安全信息和事件管理(SIEM)等工具以及威胁情报共享、用户培训和意识等计划，在减少或消除内部风险方面为企业平均节省了 300 万美元。[4]

节约 300 万美元的成本

UBA、PAM、SIEM 等工具以及威胁情报共享、用户培训和意识等项目，在减少或消除内部风险方面为企业平均节省了 300 万美元。[4]

4. https://securityintelligence.com/posts/gaining-insight-into-the-ponemon-institutes-2020-cost-of-insider-threats-report/

证据的缺乏以及 X-Force 调研中的未知因素

对于发现方式为“未向 X-Force 报告”或“缺乏证据”的内部威胁事件，X-Force 事件响应团队未得到足够的信息来进行判定。 这通常是因为许多企业的基本环境及其运行方式缺乏可视化管理。 为了检测系统内的异常活动，了解正常活动的特征至关重要，这样才能更加容易且确信可发现异常值。 2019 年，IBM 赞助了一项 SANS 研究报告[5]，该报告旨在研究企业或机构所面临的高级威胁。 该研究表明：

— 48% 的企业认为，自身基础架构缺乏可视化管理是其在安全方面的首要不足之处。

— 35% 的企业认为，对于公司内部人员滥用访问权限的情况，他们缺乏相关的检测能力。

— 47% 的企业承认，他们缺乏能力了解其网络内正常基本活动的特征。

5. https://www.ibm.com/account/reg/us-en/signup?formid=urx-39989

特权级访问权限与管理员访问权限

在分析内部威胁事件时，X-Force 划分了两种不同类型的用户。

特权用户是指企业内拥有敏感数据访问权限的人。 此类数据可能是知识产权、客户数据或人力资源信息。 这些用户也可能拥有敏感商业信息（如并购数据或其他法律信息）的访问权限。

拥有**管理员访问权限**的用户，也称管理员或网管，是指对网络内的 IT 系统拥有高级别访问权限的人。 理论上 这种访问权限不应该重叠。 然而 X-Force 发现，最终用户在其 IT 环境中可能往往是被过度赋权的状态。

拥有管理员访问权限的内部人员不同于拥有公司环境敏感访问权限的内部人员。他们当中包括拥有企业 IT 环境访问权限，并因网络特权级别高而可能对企业构成特定风险的员工、承包商/供应商。

拥有特权级访问权限的岗位实例

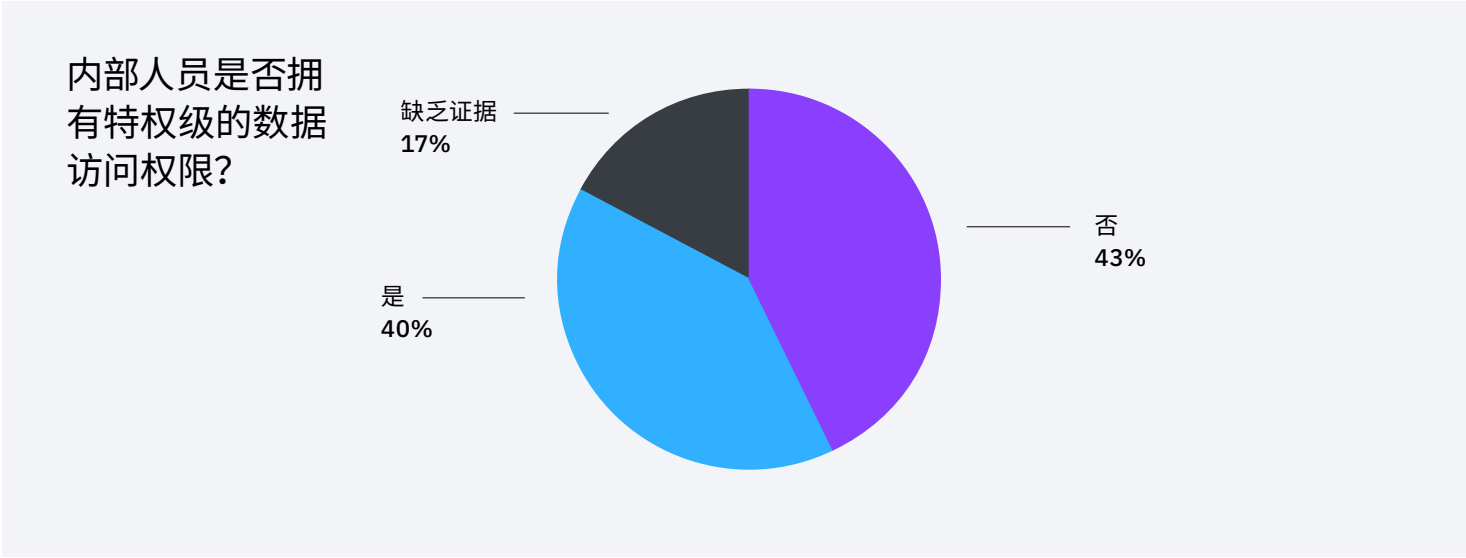
- 人力资源岗位
- 高级管理人员
- 财务岗位
- 法务岗位
- 研究职位
- 有权访问企业的知识产权、“顶尖或核心的业务”或客户数据的其他岗位

拥有管理员访问权限的岗位实例

- 服务器管理员
- IT 管理员
- 技术支持
- 第三方 IT 供应商
- 能够修改 IT 系统配置/设置的其他岗位

监督者由谁来监督?

引发事件的内部人员通常是否拥有特权级访问权限?
答案是肯定的。



X-Force 数据分析表明，在内部人员引发的事件当中，有 40% 涉及到对公司敏感资产享有特权级访问权限的员工。 在这项研究中，X-Force 将拥有特权级访问权限的人员划分为以下几种：在 IT、人力资源、财务或安全部门工作的人员或高管人员。

在另外 17% 的事件中，我们不清楚内部人员是否拥有特权级敏感数据访问权限，这意味着拥有特权级访问权限的用户所引发的事件数量实际上可能要多得多。

相比特权较为有限的人员，对关键资产（如网络共享、安全设备、电子邮件系统、员工或客户个人身份信息(PII)、知识产权或财务数据）享有高级别访问权限的个人可构成明显更高的风险。

相比访问权限较低的意外事件内部人员，由拥有特权级访问权限的意外事件内部人员导致的事件最终会给企业带来更大损失，这一点就容易理解了。 对于特权级访问权限更高的恶意内部人员，其引发的事件会造成更大的损失，涉及此类用户的攻击可能升级为全面的数据泄露。 例如，2018 年，一名为当地知名中介机构工作的澳大利亚籍房地产经纪人被判定，其在离开该机构之前访问机密数据库的罪名成立。 该经纪人通过对潜在客户的意向进行降级来操纵系统中潜在销售量的状态。 此外，该经纪人还承认，他将不当获取的 200 多份客户记录转至一家新的中介机构，用于招揽业务。 据估计，这起内部攻击事件使受害的中介机构蒙受了 3,000 万美元的潜在房地产销售损失。[6]

要防范与访问权限相关的内部事件，一种最佳方法是遵守最低特权原则，并确保用户只拥有为企业履职所需的最低访问权限。 它可以通过特权访问管理(PAM)解决方案的形式来实施，该解决方案可建立在零信任模式的基础上。[7,8] 该模式旨在让拥有用户帐户的每个人都获得尽可能少的特权，从而降低内部人员意外访问数据或资产的可能性。 在云存储领域这一理念更加重要，因为云存储涉及的数据量更大，人为和非人为的请求都需要访问此类数据才能正常运转。

在 “内部威胁在 2020 年制造的代价： 全球报告” 一文中显示，只有 39% 的企业在其内部采用了某种形式的特权访问管理模式。[9] 此外，该报告还表明，采用 PAM 方法可节省 310 万美元的成本，凸显了这些措施的有效性。

39%

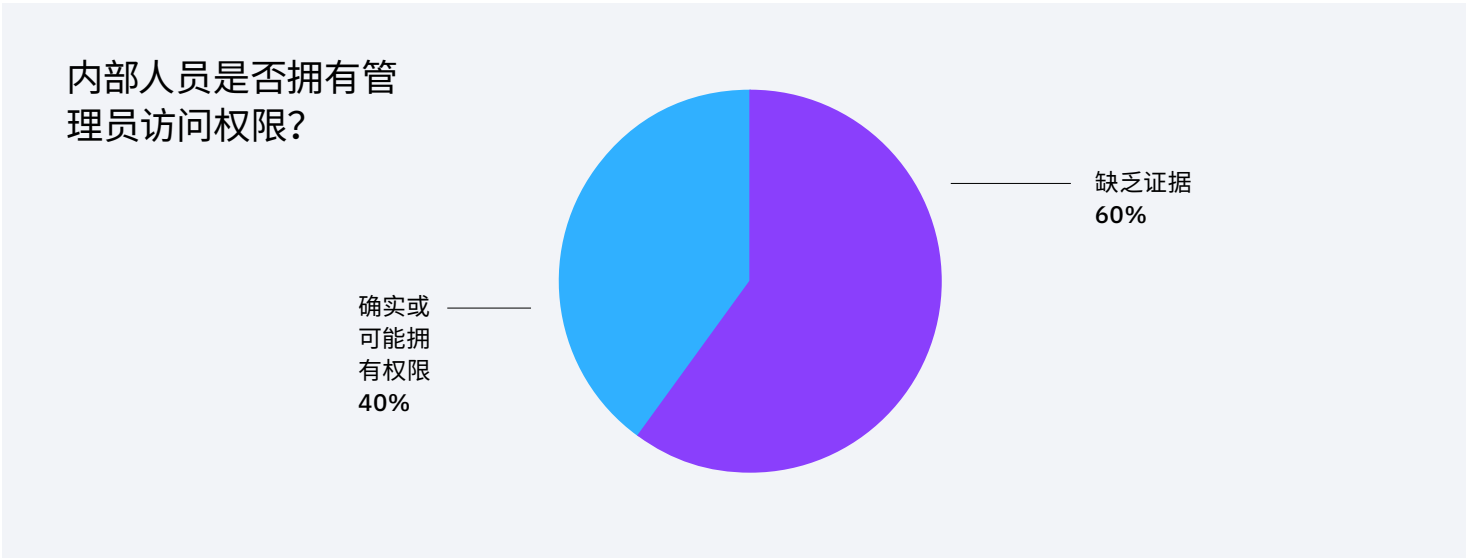
39% 的企业在其内部采用了某种形式的 PAM 管理模式。[9] 采用这种管理模式节约了 310 万美元的成本。

6. https://indaily.com.au/news/2018/10/23/harris-director-resigns-from-top-real-estate-post/
7. https://www.ibm.com/security/identity-access-management/privileged-access-management
8. https://www.ibm.com/security/zero-trust
9. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/

滥用管理员访问权限是一个代价高昂的问题

在许多公开的案例中，企业内部人员滥用其管理员权限来达到各种恶意目的，包括报复、获取金钱利益或实施诽谤等。 2020 年 2 月，前微软工程师 Volodymyr Kvashuk 被判定，其利用特权级访问权限窃取该公司价值高达 1,000 多万美元数字资产的罪名成立。[10] 案发之时，Kvashuk 负责管理一个零售平台，盗窃行为正是其利用自己在该平台上的管理员访问权限施行的。[11] Kvashuk 的具体作案手法是，使用同事的电子邮件地址和系统的有效测试帐户来混淆他们的活动，包括截留窃取数字礼品卡等。 这些礼品卡和其他被盗资产被其在互联网上转售以获取个人收益，该工程师后来利用这些收益购买了一套价值 160 万美元的房屋和一辆价值 16 万美元的特斯拉汽车。[12]

管理员访问权限被滥用的统计数据

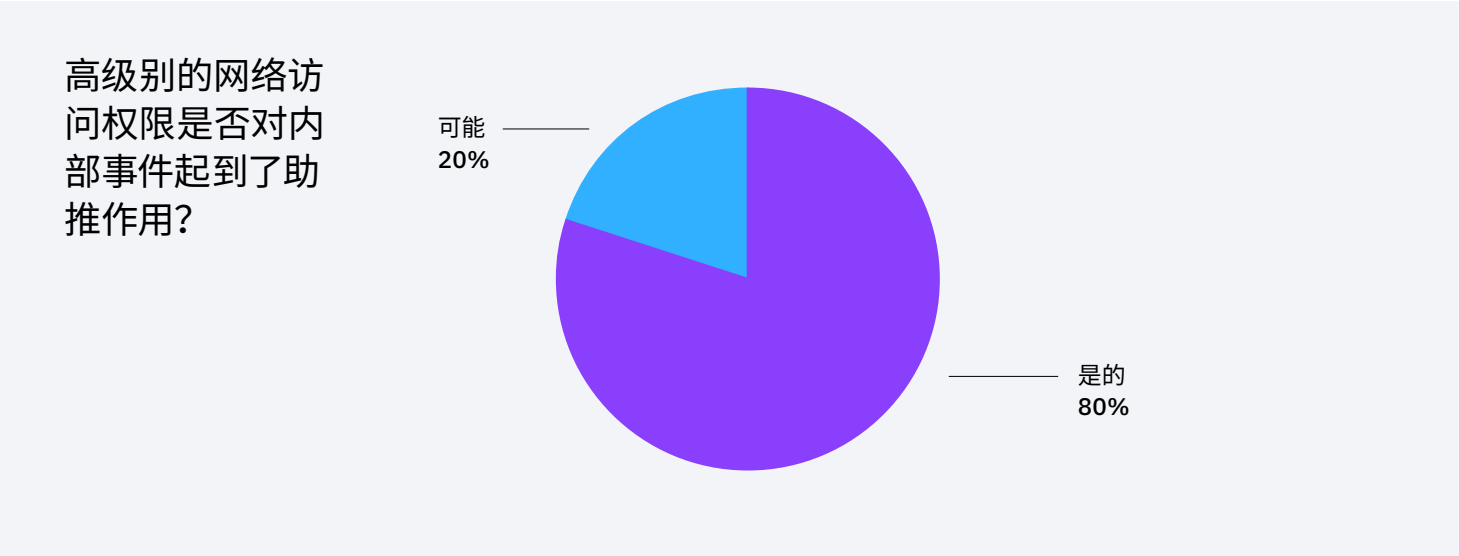


在 X-Force 从 2018 到 2020 年期间回应的 40% 的事件中，内部人员确实或可能拥有网络管理员访问权限。 在客户并未透露用户具体岗位的情况下，X-Force 分析师根据事件详情确定了内部人员访问权限的类型。

10. https://www.justice.gov/usao-wdwa/pr/former-microsoft-software-engineer-sentenced-nine-years-prison-stealing-more-10-million
11. https://apnews.com/article/seattle-retail-sales-james-robart-13f5a86053533b40034246ef37ecad8d
12. https://www.redmond-reporter.com/news/former-microsoft-employee-convicted-of-18-federal-felonies/

这些事件涉及数据渗漏、敏感数据的泄露和删除，以及安装未经授权的软件等。 具体事例包括，一些企业的服务器丢失了数千万亿(petabyte)字节的日志、遭受蓄意导致的源代码泄漏，或者因具有管理员访问权限的内部人员的不当操作而遭致代价高昂的停机事件。

更值得关注的一点是，在内部人员确实或可能拥有管理员访问权限的事件中，100% 的事件都遭受这种高级别访问权限的影响。 （见下图）



换个角度来看：如果内部人员没有管理员访问权限，那么，事件对企业的影响可能会小得多，或在许多情况下根本就不会发生。 X-Force 已对多起服务器遭遇关键数据库和日志被删除的内部事件做出响应。 如果内部人员没有这些系统的管理员访问权限，事件就不会发生。

建议

X-Force 认为，内部事件的数量在第三方数据中被低估了。 可能还有更多此类性质的事件被企业在内部处理了，因担心招致承担责任或声誉受损而未公布。[13]

X-Force 的研究结果和数据强调，基于这些事件可能对企业造成的影响，潜在的内部威胁需要纳入信息安全计划，构成其中重要的组成部分。 具体而言，IBM Security 针对内部威胁提供了以下建议：

纵深防御策略可以很好地检测内部威胁。

对企业的技术和流程实施多层管理的做法，历来被认为是为了应对外部威胁。然而，X-Force 的研究结果表明，此处涉及的许多工具（包括安全信息和事件管理(SIEM)解决方案）在检测内部威胁活动方面也发挥了重要作用。

了解自身环境中哪种状态是正常的。

要检测任何类型攻击者的可疑活动，最佳方法是了解你们网络中哪些类型的活动属于正常范畴。 对基本活动的深入了解有助于及时、有效地检测和应对异常行为。 一套健全的用户行为分析(UBA)解决方案可以提供这种功能，还可以随时间的推移而适应环境变化。

定期审查管理员访问权限。

X-Force 发现，若干起涉及管理员的内部事件可能是由于用户的特权级别过高而造成的。 应围绕管理员访问权限实施严格的调整和过程控制，尤其是负责关键任务的服务器访问权限。 考虑技术型解决方案，通过这种方案来授予敏感系统及功能的临时 管理员访问权限，并做好相关记录。

13. https://www.darkreading.com/edge/theedge/fbi-encounters-reporting-an-insider-security-incident-to-the-feds-/b/d-id/1340016

将信息安全团队和 IT 管理员团队分开。

X-Force 的经验表明，以相互制衡的方式对安全团队和管理员团队进行独立性和治理方面的管理，有助于改善安全环境。 这种方式还能让管理员团队具备必要的灵活性和创造力，以优化其对威胁的探索和发现，同时为企业提供充分的监督，从而最大程度地降低团队内的风险。

为企业内的敏感岗位建立风险预测机制。

由于高级别访问权限在 X-Force 响应过的许多内部事件中会造成影响，因此我们建议，企业可以考虑对其内部拥有系统或数据敏感访问权限或管理员访问权限的职位建立风险预测机制。 实施一套围绕零信任模式构建的特权访问管理(PAM)解决方案后，用户得到的特权级访问权限将被控制在最低水平，从而将内部事件的影响降至最低。

更新事件响应方案，将内部威胁囊括在内。

对于此类事件，普通培训是不够的。 虽然大多数事件响应方案针对的是外部对手的攻击，但组织应当考虑添加情境，将意外或恶意的内部威胁情境囊括在内。 找到一个可以帮助制定“事件响应计划”和攻击应对方案的合作伙伴，以更有效地针对网络攻击进行准备和应对。

持续培训员工。

合乎道德规范的商业实践被许多企业纳入其年度培训计划以及社会工程培训中。X-Force 响应过的许多内部事件都是由其他员工发现的，而不是通过技术手段。企业应在年度商业道德或社会工程培训活动中纳入可疑内部事件的报告模式。此外，对拥有特权级访问权限的员工需针对其岗位职责进行培训，有助于他们对周围出现的一些泄密迹象保持清醒认识。

充分发挥声誉良好的威胁情报机构的服务能力。

客户经常会在创建、管理和使用威胁情报方面遇到挑战。寻求一种具备聚合、自动化及整合功能的解决方案，以满足大规模使用威胁情报的需要。

托管检测和响应服务为您提供全天候保护。

托管检测和响应(MDR)型安全服务对预防、检测和快速响应内部威胁而言至关重要。 采用新一代 AV 技术开展基于行为的拦截、调查和持续策略管理，超越传统防范措施的解决方案是计划的关键。

了解 IBM Security 如何帮助客户保护高度复杂和重要的环境，使其免受外部和内部威胁。

了解有关 IBM Security 的更多信息

IBM Security

国际商业机器 (中国) 有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编: 100020

美国出品
2021 年 5 月

IBM