面向各级员工的网络安全技能

卡巴斯基安全意识

kaspersky 引领未来

如需了解更多信息，请访问
kaspersky.com.cn/awareness

卡巴斯基安全意识
在整个组织中建立网络安全文化

超过 80% 的网络安全事件由人为错误造成。通过在整个组织中建立网络安全行为文化，并培养员工的基本网络安全技能和意识，您可以减少攻击面和必须处理的事件数量。要解决网络安全中的 “人为因素” 问题，就必须改变员工的行为方式，最有效的办法便是开展培训，采用最新的成人教育技术和技巧，并提供最相关和最新的内容。

人为因素 - 网络安全中最薄弱的一环

网络安全解决方案正在迅速发展并适应复杂的威胁，这加大了网络罪犯攻击得逞的难度，因此这些罪犯开始攻击网络安全中最薄弱的一环，即人为因素。

55% 的公司报告其员工违反了 IT 安全政策*

43% 的小企业报告称员工违反 IT 安全政策导致安全事件**

数据泄露是最常见的安全问题，通常因**员工** (22%) 和攻击者 (23%) 导致。*

30% 的员工承认，
自己会与同事分享办公电脑的登录名和密码详细信息***

23% 的组织没有为企业数据存储制定任何网络安全规则或策略***

卡巴斯基安全意识 – 掌握 IT 安全技能的全新方法

卡巴斯基安全意识是一款久经考验、行之有效的高效解决方案，其成功获得了全球客户的广泛认可。该解决方案将卡巴斯基超过 25 年的网络安全经验与在成人教育方面的深厚积累相结合，其用户分布在超过 75 个国家/地区，由不同规模的企业用于对 100 多万名员工进行培训。

它提供了一系列生动有趣且有效的培训解决方案，可提高员工的网络安全意识，使他们能够各尽其责，帮助组织提升整体网络安全水平。由于可持续的行为变化需要时间，我们的方法涉及到构建具有多个组成部分的持续学习周期。

持续学习周期

1 参与/动力
- 我为什么需要它?
- 认知

2 起点
- 我具备相关意识吗?
- 我都了解些什么，差距在哪里?

3 学习
- 微学习
- 持续学习
- 应变能力

4 整合
- 我做对了吗?
- 我还记得这件事吗?
- 我有相应地采取行动吗?

培训计划的重要差异化优势

丰富的网络安全专业知识

我们的网络安全技能源自超过 25 年的网络安全相关经验，这种底蕴是我们产品的核心

改变组织各级员工行为方式的培训

我们的游戏化培训采用寓教于乐的方式，吸引员工参与、激发员工动力，而学习平台则有助于吸收理解网络安全技能集，以确保员工不会边学边忘。

* 《2022 年 IT 安全经济影响分析》，卡巴斯基

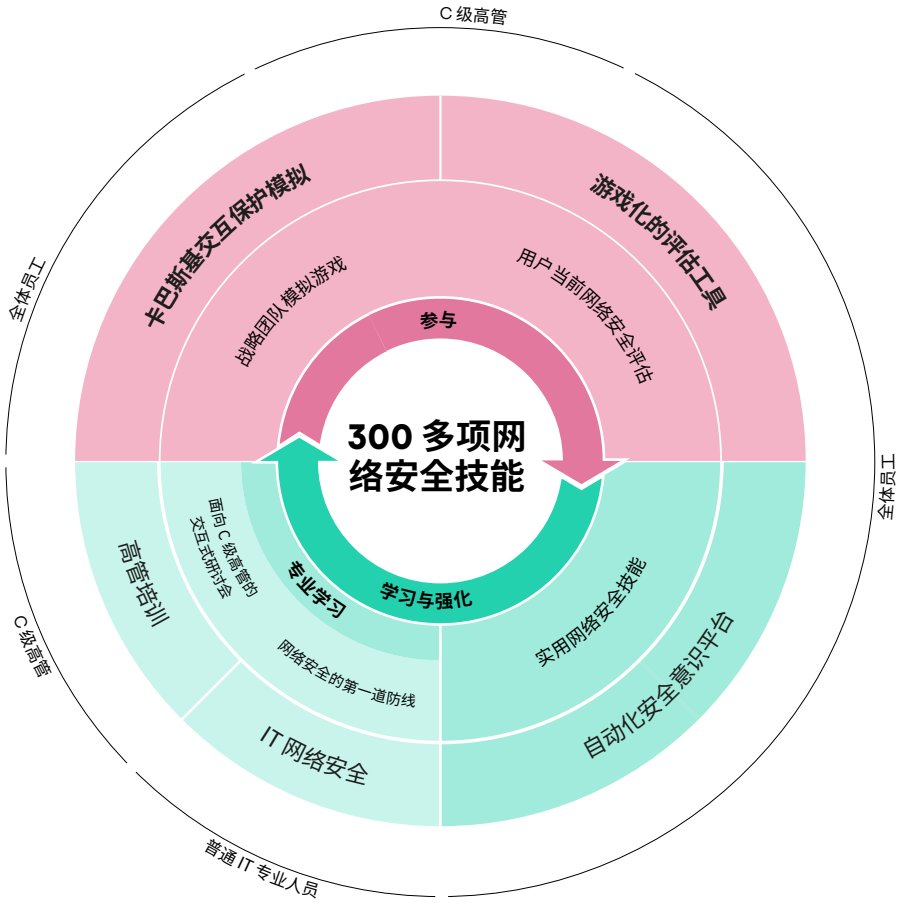
** 《2021 年 IT 安全经济影响分析》，卡巴斯基。

*** 《理清混乱数字环境的千头万绪》。卡巴斯基实验室，2019。

激发树立有效的安全意识的动力

改变员工行为方式是您最大的网络安全挑战。人们往往没有动力去掌握技能并改变习惯，因此许多为教育付出的努力最后只是流于形式。有效的培训囊括众多不同的环节，应该考虑到人性特点和吸收理解技能的能力。作为网络安全专家，卡巴斯基知晓能保证网络安全的用户行为该是怎样的。我们运用自身的深入见解和专业知识，增加了学习技巧和方法，让客户的员工能够抵御攻击，同时让他们无拘无束地自由发挥。

面向不同组织级别的不同培训形式



员工失误，组织买单...

52.887 美元
每个企业组织
员工因使用 IT 资源不当招致网络攻击给企业造成的平均财务损失*

30%
的恶意软件攻击
是通过带虚假链接和附件的电子邮件实施的**

79%
的员工
承认，在一年内，尽管意识到了隐患，也至少有过一次存在风险的活动***

164 美元
每条记录
涉及 2,200 至 102,000 条记录的数据泄漏的全球平均成本****

42% 的供职于超过 1000 名员工的公司的受访者
表示他们所参加的大多数培训计划既不实用，又非常无趣*****

* 《2022 年 IT 安全经济影响分析》，卡巴斯基
** 《数据泄露调查报告 - 2022年》
*** 《平衡风险、生产力和安全性》，Delinea，2021 年
**** 《数据泄露的成本 - 2022年》。IBM
***** Capgemini，《数字人才缺口》

卡巴斯基安全意识解决方案

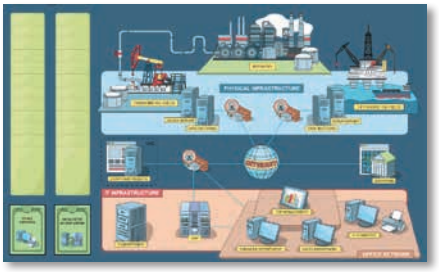
参与/动力

员工并非总是热衷于强制性的培训，而且在网络安全方面，许多人认为培训过于复杂或无聊，或者认为与他们毫无关系。如果没有学习的动机，就没法取得十分积极的学习成果。对于负责教育的人来说，另一个挑战是让企业高管参与培训，尽管他们的失误给公司带来的损失可能与其他人一样大。这就是游戏化方法的用武之地，这种方法颇具吸引力，所以是鼓励员工克服最初对培训的抵触情绪的最有效方法。

76% 的首席执行官承认他们为了更快完成任务，会绕过安全协议，以牺牲安全为代价来换取速度*。

62% 的管理人员承认，因组织内部在 IT 安全方面的沟通失误，引发了至少一次网络安全事件**

KIPS 培训面向高级管理人员、业务系统专家和 IT 专业人员，以提高他们对使用各种 IT 系统和流程所带来的风险和挑战的认识。



卡巴斯基交互式保护模拟 (KIPS)：立足企业视角审视网络安全

KIPS 是一款游戏时长 2 小时的互动式团队游戏，能够建立决策者（资深业务高管、IT 高管和网络安全高管）之间的理解，并改变他们对网络安全的看法。它通过软件模拟的方式，展示了恶意软件和其他攻击对业务绩效和收入的实际影响。它促使玩家进行战略性思考、预测攻击的后果，并在时间和财务资源的限制下作出相应的响应。每一项决策都会影响所有业务流程，而主要目标是保持一切平稳进行。完成游戏时收入最高，同时发现并分析了网络安全系统中的所有陷阱并作出适当响应的团队将获胜。

13 个行业相关场景（我们还会不断添加更多场景）

每个场景都展示了网络安全在业务连续性和盈利能力方面的作用，突出了新出现的挑战和威胁，以及组织在构建网络安全时所犯的典型错误。它还能促进了业务与安全团队之间的合作，有助于维持稳定的运营和应对威胁的可持续性。

KIPS 提供两种版本：

极受欢迎的 KIPS Live 版本采用了现场面对面的竞赛形式，营造出一种令人热血沸腾的氛围。它是在组织内参与和建立网络安全文化的绝佳工具。

在 KIPS Online 版本中，用户可以与来自任何地区的大量参与者进行互动。KIPS Online 非常适合全球性组织或公共活动，可以与 KIPS Live 结合使用，让远程团队参与到现场活动中。

- 支持多达 300 个团队（约 1000 名受训人员）同时参与，地点不限。
- 不同的团队可以选择不同语言的游戏界面。
- 客户可以从库中选择游戏中的攻击数量和类型，对预先设定的场景进行个性化设计。
- Online 版本的另一个优势是可以获取有关玩家选择的统计数据、团队在某些情况下的操作数据以及前一轮游戏的玩家操作基准。

面向企业的 KIPS

拥有许可证的客户可以在许可证有效期内随心畅玩 KIPS，他们可以按照预定义的设置玩游戏，也可以在每次玩游戏时对游戏场景进行个性化设置，从库中选择不同的攻击并组合到一起。个性化设置功能可以改变每次游戏的玩法，让游戏变得更加有趣。

---

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speakfluent-infosec-2023/

起点

人们通常不知道自己究竟有多无知，这使他们特别容易受到伤害。他们需要接受测试，需要获得有关其网络安全能力水平的详细、明确的反馈，以便进一步提高培训效果。这还可以确保人们不会将时间浪费在自己已经熟悉的材料上。

游戏化评估工具：评估员工网络安全技能的快捷、有趣方法

卡巴斯基游戏式评估工具(GAT) 让您可以快速评估员工的网络安全知识水平。引人入胜的互动式方法杜绝了传统评估工具普遍存在的乏味无聊。员工只需 15 分钟就能经历 12 个与网络安全相关的日常情景，评估游戏角色的行为是否有风险，并表明对自己所做响应的自信程度。

完成后，用户将收到一份证书，其分数体现了他们的网络安全意识水平。他们还会获得其中各个领域的反馈，包括解析和实用提示。

GAT 的游戏化方法能够激励员工，而且能通过让员工应对某些网络安全情景，展示其知识可能存在欠缺。这也有助于信息技术/人力资源部门更好地了解其组织内部的网络安全意识水平，此外也可以作为更广泛的教育活动的入门步骤。

学习

我们的在线学习平台是安全意识培训计划的核心。它包含**超过 300 项网络安全技能**，涵盖所有主要的 IT 安全主题。
每节课都包括案例和真实示例，能够让员工联系到自己在日常工作中必须处理的问题。在第一节课结束之后，他们可以立即将这些技能付诸应用。

卡巴斯基自动化安全意识平台：高效便捷的培训管理，适合任何规模的组织

卡巴斯基 ASAP 是一款有效且易用的在线工具，可培养员工的网络安全技能，并激发他们以正确的方式行事。

尽管培训可满足所有公司的安全意识需求，但自动化管理将特别吸引那些没有专门培训管理资源的公司。

主要优势：

- **通过完全自动化实现简化：** 可以轻松启动、配置和监控培训计划，而且持续管理是完全自动化的，无需管理员参与。该平台本身为每组员工设定了教育计划，通过各种培训形式自动提供间隔式学习。
- **简化管理员操作：** 自动化平台管理、与 AD (Active Directory) 同步、SSO（单点登录）、Open API（与第三方解决方案交互的能力）、使用方便的仪表板、首次访问时的在线用户引导、常见问题解答部分和提示，均让平台管理变得方便高效。
- **方便学员使用：** 清晰的课程结构、微课程、真实案例、使用方便的界面、电子邮件提醒、可以重新学习和反复学习的课程设计、支持 PC 或移动设备的界面——所有这些优势让学习过程变得愉快、有趣且高效。

卡巴斯基 ASAP：一种易于管理的在线工具，可逐级培养员工的网络安全技能水平

ASAP 中涵盖的主题：

- 密码和帐户
- 电子邮件
- 网站和互联网
- 社交媒体和即时通讯软件
- PC 安全
- 移动设备
- 保护机密数据
- 通用数据保护条例
- 工业网络安全
- 个人数据
- 银行卡安全和 PCI DSS
- 人肉搜索
- 加密货币安全
- 远程办公时的信息安全
- 俄罗斯第 152-FZ 号联邦法律

ASAP 快捷课程

音视频格式的简短培训。

- 交互式理论
- 视频
- 测试

卡巴斯基 ASAP 是一款多语言版本的解决方案。

ASAP 是 MSP 和 xSP 的理想选择 – 多个业务的培训服务可以通过一个帐户进行管理，并且可以按月订阅授权许可。

访问 asap.kaspersky.com，体验完整功能版本的卡巴斯基 ASAP，亲眼见证设置和管理自己的企业安全意识培训计划是多么轻松！

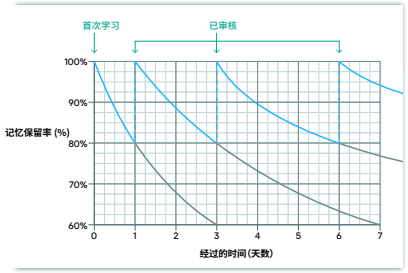
整合

强化是学习计划的重要组成部分，也是巩固学习阶段获得的知识和技能所必不可少的环节。

将学习技能转化为习惯的最佳方法是实践。有些时候，人们会犯错，并通过个人经历学习进步。但在网络安全方面，从错误中汲取经验的代价可能十分高昂。

通过游戏化培训，您可以栩栩如生地“体验”一种实际情景并了解其后果，而且不会给您自己或您的公司造成任何损失。

70%
的所学知识
会在一天内遗忘（在传统培训形式中）



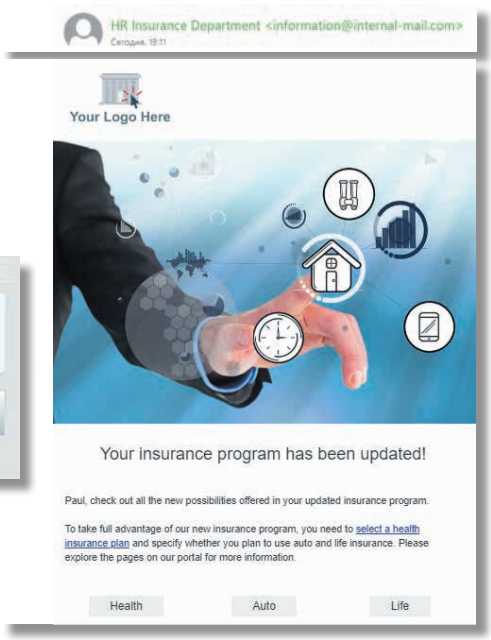
- **达到期望的学习效率：**计划内容的结构旨在支持循序渐进的间隔式学习，并持续强化巩固。这种方法基于人类记忆的特性，以确保知识的保留和随后的技能应用。
- **定制：**可以轻松更改培训计划的外观——在管理员和学员门户以及平台电子邮件中将卡巴斯基徽标替换成您公司的徽标；定制证书，并在任何课程中添加个性化内容。
- **灵活的学习：**选择适合您的员工培训方案：可以向员工分配一门基本的**快捷课程**，帮助您快速满足网络安全培训的监管要求，或者更新他们的知识；也可以选择按复杂程度细分的**主要课程**，以展开更细致深入的网络安全技能培养。
- **灵活的授权许可**（针对托管服务提供商）：按用户许可的模式提供，可购买最低 5 个授权许可，并且可以用一个帐户管理多家公司。

模拟网络钓鱼活动

模拟网络钓鱼攻击可以在培训之前、期间和之后使用，以测试员工抵御网络攻击的能力，并帮助他们和公司管理层看到培训的好处。

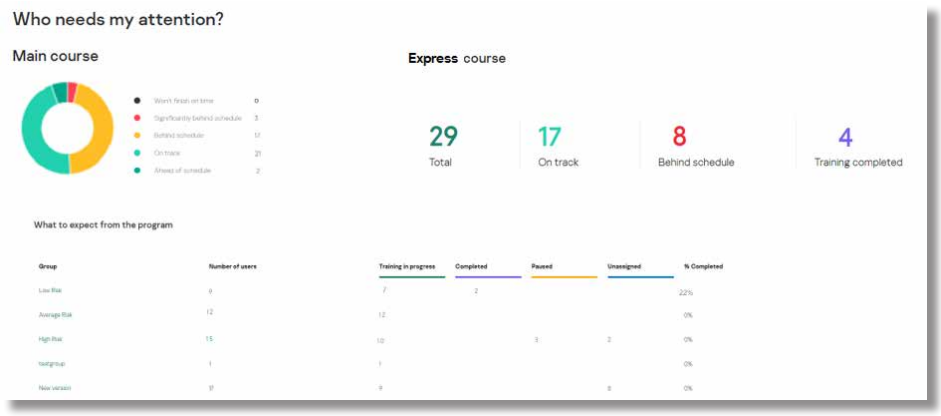
互动课程

模拟网络钓鱼攻击



跟踪成效

您可以通过仪表板关注员工的进展情况，一目了然地评估整个公司和各组取得的进步。您还可以深入了解个人层面的更多细节。



专业学习

普通 IT 专业人员：帮助台人员和其他精通技术的人员经常被排除在培训之外，因为标准的安全意识培训计划对他们来说不够，但公司也不需要将他们变成网络安全专家：这太昂贵、耗时且没有必要。

我们很高兴地告诉大家，我们的培训填补了这一空白——没有专家培训那么深奥，但比普通员工的培训更高级。

CITO 培训模块：

· 恶意软件
· 潜在有害的程序和文件
· 调查基础
· 网络钓鱼事件响应
· 服务器安全
· Active Directory 安全

CITO 交付方式：

云或 SCORM 格式

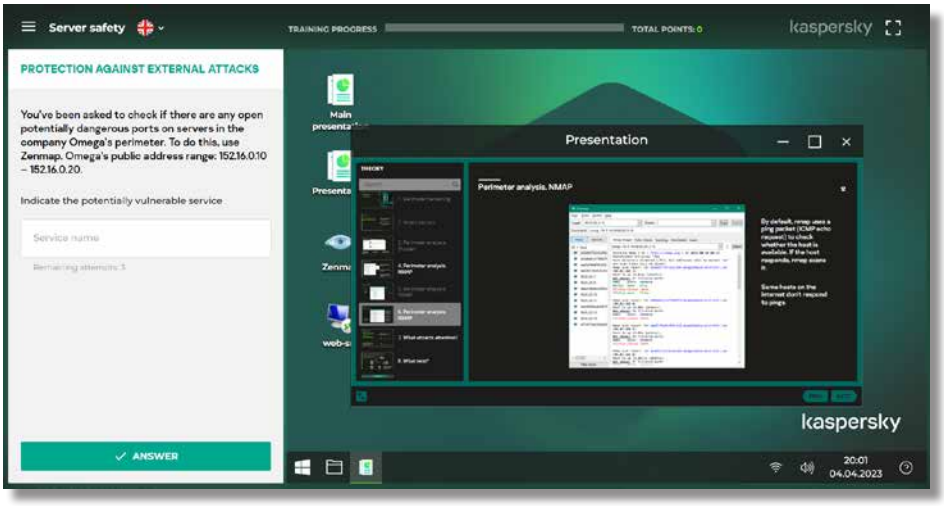
IT 在线网络安全：第一道事件防线

IT 在线网络安全是面向所有 IT 相关人员的互动式培训。它能为网络安全和一级事件响应技能打下稳固基础。

该计划可为 IT 专业人员提供实用技能，以识别表面看起来良性的 PC 事件中可能存在的攻击场景。它还能培养搜寻恶意征兆的意愿，巩固所有 IT 团队成员作为第一道安全防线的角色定位。

CITO 还教授调查基础知识以及如何使用 IT 安全工具和软件，以便为您的 IT 专业人员掌握理论、增加实践，通过练习提高技能，从而使他们能够收集事件数据以移交给 IT 安全部门。

我们建议您组织内的所有 IT 专家（主要是帮助台和系统管理员）参加此培训。大多数非专家 IT 安全团队成员也能从本课程中受益。



让高管加入进来

高级管理人员是网络犯罪分子最渴求的目标之一，但他们往往是教育工作者面临的真正挑战。然而，如果没有他们的参与和对各种网络安全倡议和倡导的支持，就不可能在组织中建立网络安全文化。

网络安全与项目管理、金融工具和业务运营效率一样，是创收的一个重要方面。这是我们高管课程的重点。

高管培训：

在我们的高管培训计划中，业务领导和高层管理人员通过导师主导的互动研讨会或在线课程来学习网络安全的基础知识，使他们更好地了解网络威胁以及如何进行防范。

该培训重点关注网络安全对公司财务的影响和投资的可行性，帮助 C 级高管更好地理解网络安全与经营效率之间的联系。他们将了解当前的威胁形势对公司的影响，在遭遇网络攻击时应采取的行动，以及许多其他有趣、相关且实用的信息。

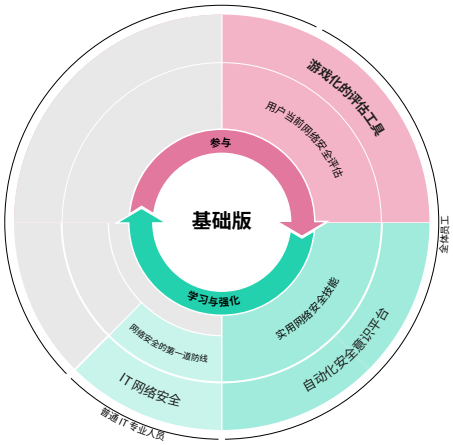
为了发挥该课程的更大价值，最好将其与 KIPS 培训结合使用。根据您的安全意识方法，可以在 KIPS 之前或之后进行高管培训。

* 如需查看当前模块列表，请访问 cito-training.com

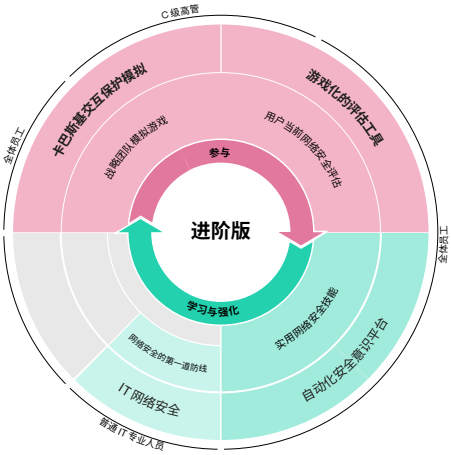
卡巴斯基安全意识: 灵活的培训方式

卡巴斯基培训解决方案涵盖您公司的各个层面，可以单独使用，也可以结合使用。我们还根据您的需求量身定制了套餐，让您能够更轻松地启动培训计划。

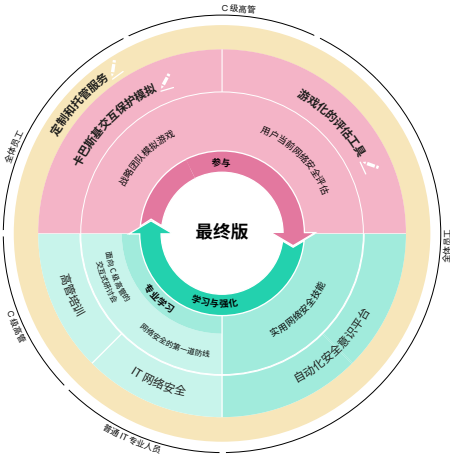
提高员工网络安全意识的无忧之选，设置简单，管理方便。
提供基本级别的安全培训，帮助您成功运营并满足监管或第三方对一般网络安全培训的要求。



使用简单的“交钥匙”培训解决方案帮助大型组织保持业务连续性。通过覆盖学习周期的每个阶段来支持每个组织级别并改变其行为。



最大程度地确保网络安全意识，以定制和托管服务为特色，以便高管精通威胁场景，员工具备自动网络安全技能，普通 IT 员工作为第一道防线为您提供支持。



卡巴斯基安全意识培训使用最新的培训方法和先进的技术来确保成功。灵活的新套餐式解决方案可以根据您的需求量身定制，从而为每个人提供适合的解决方案。如需了解更多信息，请访问 kaspersky.com.cn/awareness

卡巴斯基安全意识: kaspersky.com.cn/awareness
IT 安全新闻: business.kaspersky.com.cn/

kaspersky.com.cn

kaspersky