卡巴斯基交互式保护模拟

树立高层管理人员和决策者的网络安全意识

kaspersky 引领未来

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

卡巴斯基交互式保护模拟

“人员问题”

当今企业面临的最大安全挑战之一在于，不同的高级管理人员从不同的角度看待网络安全，工作重点也不同。这可能导致企业在决策上陷入“三足对立”的局面：

- 企业管理人员认为安全措施与他们的业务目标（成本更低/速度更快/质量更好）相悖。
- IT 安全经理可能会认为，网络安全属于基础设施和投资问题，不在他们的职权范围内。
- 而负责成本控制的管理人员可能只看到网络安全会产生成本，却没有意识到这方面的支出与创造收入和节约成本的关系。

这三方面的管理人员要相互理解，密切合作，这对于促进网络安全的有效性是至关重要的。然而，讲座和红蓝对抗演习这类传统的安全意识活动存在缺陷：耗时很长、技术性强，不适合忙碌的管理人员，而且无法建立一种“通用语言”。

C 级高管站在公司网络安全防御的第一道防线

对于当今的许多公司来说，维护其 IT 基础设施的可持续性是当务之急。然而，网络安全问题通常由 IT 和 IT 安全人员负责，这可能会在企业内部形成一种各自为政的网络安全行为文化。企业领导者主要关注销售业绩、客户体验、风险和成本，在努力实现这些目标的同时往往会忽视网络安全。但如果没有高层管理人员的积极支持和以身作则，就无法形成统一的网络安全文化。

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**。

51% 的信息安全工作人员认为商讨增加 IT 安全预算是最难的，但对于可行的沟通策略持一致意见。

大多数 C 级高管 **(56%) 和 IT 工作人员 (48%)** 一致认为，提供真实案例是简化 IT 安全相关问题沟通的最有效方法**。

卡巴斯基安全意识解决方案如何发挥价值

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卡巴斯基学院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**。

这套解决方案由生动有趣的培训产品组成，可以提高各级员工的**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。

其中的每一款产品在整个学习周期中都发挥特定的作用，而且都可以单独提供。

面向高管的战略性网络安全运营游戏

卡巴斯基交互式保护模拟 (KIPS) 侧重于战略性的业务模拟，是一款团队游戏，展示了业务效率和网络安全之间的联系。

参与者置身于一个模拟的业务环境中，扮演 IT 安全团队成员的角色。他们会遇到一系列意想不到的网络威胁，同时必须维持公司的平稳运营并赚取收入。

他们要从可用的最佳主动和被动控制措施中进行选择，从而建立网络安全防御策略。他们所做的每一项选择都会改变场景的展开方式，并最终影响公司获得或者损失多少收入。

团队在现实网络攻击成本，以及工程、业务和重点安全工作之间取得平衡，同时分析数据，基于不确定的信息和有限的资源做出战略决策。如果这听起来很切合实际，那是因为所有场景都是基于真实事件来设计的。

* 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/speak-fluent-infosec-2023/

KIPS 是一款动态的意识游戏，遵循“实践出真知”的理念：

- 有趣、引人入胜、迅速（2 小时）。
- 培养团队合作精神。
- 以竞赛的形式培养主观能动性和分析能力。
- 通过玩游戏来加强对网络安全措施的理解。
- 所有场景和攻击都基于真实案例

KIPS 为什么有效

KIPS 培训面向业务系统专家、IT 人员和部门经理，用于提高他们对使用现代计算机化系统所涉及的风险和安全问题的认识。

每个团队由 4-6 人组成，负责经营一项业务，其中涉及生产设施和控制这些设施的计算机。在游戏过程中，这些生产设施会产生收入、加强公众意识并取得业务成果。与此同时，团队必须应对可能影响业务绩效的网络攻击。

在游戏结束时，参与者将获得切实可行的重要见解，之后可以将这些见解应用到实际工作中。

- 网络攻击会导致收入受损，高层管理人员必须予以解决
- IT 和非 IT 决策者之间的合作对于每个企业构筑高效的网络安全防线至关重要
- 合理的安全预算并不会带来过高的成本，但网络攻击一旦得逞就会导致收入受损
- 人员能够很快适应安全控制措施并意识到这些措施的重要性（审计培训、反病毒软件等）

KIPS 提供两种版本：

极受欢迎的 **KIPS Live** 选项营造了一种令人热血沸腾的氛围，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**，用户可以在任何方便的地方与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。
- 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。
- 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。

KIPS 揭示了：

- 网络安全在业务连续性和盈利能力方面的作用。
- 企业面临的新挑战和威胁。
- 企业在构筑网络安全时所犯的典型错误。
- 业务和安全团队之间的合作如何有助于维持稳定的运营和持续的网络威胁防护。

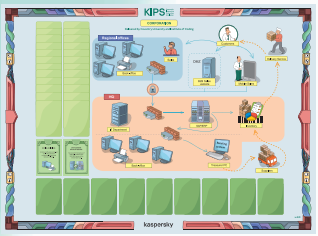
各个团队根据具体场景，负责特定行业的公司的 IT 安全。他们的任务是确保公司正常、无间断地运作，维护与客户和供应商的关系，以及发现并消除网络威胁。

在游戏过程中，当企业遭受网络攻击时，玩家会体会到生产和收入受到的影响，并学会采用不同的业务和 IT 战略以及解决方案，从而将攻击的影响降至最低，而不损失收入。

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！**

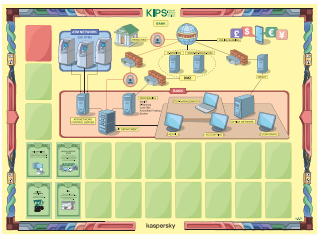
企业 KIPS 场景适用于所有垂直行业

企业



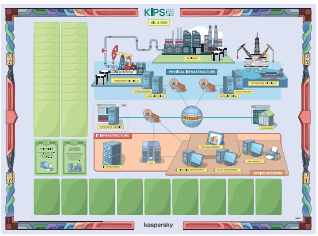
保护企业免受**勒索软件、高级持续性威胁 (APT) 和自动化安全缺陷的影响。**

银行



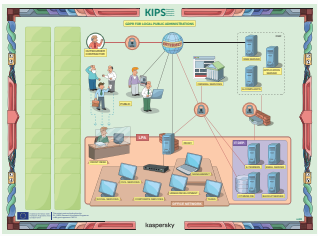
帮助金融机构抵御**高级新兴 APT，比如 Tyukpin 和 Carbanak。**

石油与天然气



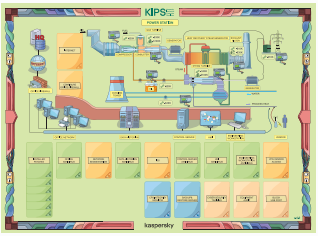
从**网站篡改到真实的勒索软件和复杂 APT，探究各种威胁的影响。**

地方行政部门



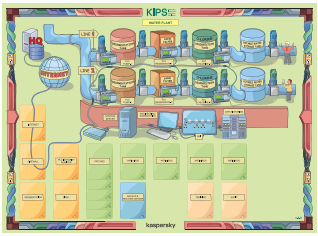
保护公共 Web 服务器免遭攻击和漏洞入侵。

发电站



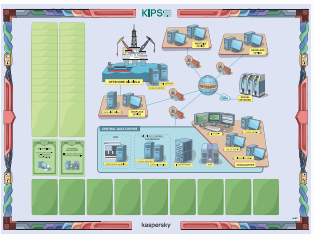
保护工业控制系统和关键基础设施免遭“震网”(Stuxnet) 式网络攻击。

水厂



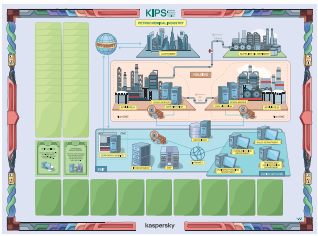
保护净水厂的 IT 基础设施，确保两条生产线的稳定运行。

石油控股



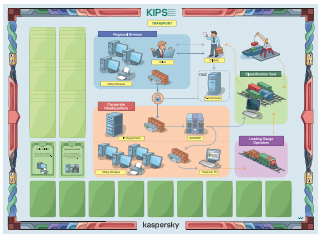
维护网络安全，为一家业务遍布全球的石油能源公司提供创收保障。

石化行业



确保专注乙烯生产的大型石化控股公司新设立的分公司正常运作。

运输

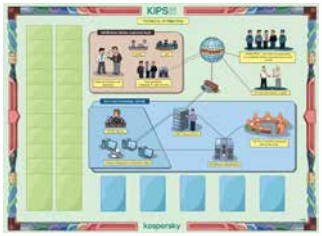


帮助物流公司抵御 **Heartbleed、APT、B2B 勒索软件、Insider。**

机场

确保机场乘客的安全和货物的及时交付，保护其资产免遭不同的网络攻击和威胁的侵害。

技术归因



调查并对联合国服务器遭遇的复杂 APT 攻击进行技术归因。

中小型企业

帮助中小型企业保护其业务免遭与分布式拒绝服务 (DDoS)、勒索软件、移动应用程序黑客攻击和身份盗窃有关的网络安全威胁。

电信

保护由电信公司、云服务商、游戏开发商和总部组成的大型电信控股公司的资产。

想要发挥出 KIPS 的更大价值吗?

您可以通过卡巴斯基安全意识产品组合中的**高管培训**来完善 KIPS 体验。根据您的安全意识方法，可以在玩 KIPS 之前或之后为管理人员提供该培训。您可以发现当前的威胁形势对业务的影响，在遭遇网络攻击时应采取的行动，以及大量其他有趣、相关且有用的信息，从而提升 KIPS 体验（高管培训有两种形式：互动式线下讲习班或在线课程）。

KIPS 用户和客户对该游戏的评价

卡巴斯基工业保护模拟解决方案真的让我大开眼界，应该成为所有安全专业人员的必备工具。

Warwick Ashford, Computer Weekly

我们欧洲核子研究中心 (CERN) 部署了大量的IT和工程系统，有数千人依赖这些系统来工作。因此，
从网络安全的角度来看，我们必须提高人们对网络安全的认识并让他们参与进来，这与技术层面的控制措施同样重要。事实证明，卡巴斯基培训是引人入胜、设计巧妙且高效的培训。

Stefan Luders, CERN 首席信息安全官

这款游戏确实令人大开眼界，许多参与者纷纷咨询如何在自己的公司使用这款游戏。

Joe Weiss PE, 注册信息安全员 (CISM)、风险及信息系统控制证书 (CRISC) 持证人、国际自动化协会 (ISA) 专业人员

我们必须建立一个基于隶属和合作关系的人际网络，而 KIPS 是完美的起点。

Daniel P. Bagge, 捷克国家网络安全中心

如何为开展 KIPS 培训做好准备

安排： KIPS 作为单独的活动，或者作为现有活动/会议/研讨会中的一个环节（在这种情况下，KIPS 最好安排在第一天晚上）。

分组： 共 20-100 人，3-4 人组团，理想情况下，每个团队都包含管理人员、工程师、CISO/IT 安全人员：
- 最好是每个角色/职能部门至少 1 人，
- 各团队可由来自不同或同一公司/部门的人员组成，
- 参与者是否相互认识并不重要。

布置： 游戏时间为 1.5–2 个小时，但卡巴斯基的协调员小组必须在游戏开始前 2 个小时内进入房间进行准备和布置。

房间： 计划面积为人均 3 平方米，无立柱，带标准影音播放设备：投影仪（6-8 流明）、屏幕、音响系统（扬声器、遥控器、麦克风）。

支持联网的 Wi-Fi（用于访问 KIPS 游戏服务器），每组（4 人）配备 iPad（网速 4Mbps，可连接 Wi-Fi）
或其他平板电脑。

家具：
4 人桌（长方形桌，尺寸不小于 75x180 厘米，或者圆桌，直径不超过 1.5 米），参与者应按 4 人一组坐在桌旁。联合主持人的桌子，为所有参与者准备的椅子。

参考资料和案例研究

KIPS 游戏得到了 50 多个国家/地区的工业安全专业人士的青睐。

- KIPS 已被翻译成英语、俄语、德语、法语、日语、欧洲西班牙语、拉丁美洲西班牙语、葡萄牙语、土耳其语、意大利语、汉语、荷兰语和阿拉伯语
- 马来西亚网络安全局、捷克国家安全局和荷兰国家网络安全中心等许多政府机构也在使用 KIPS，用于提高国家关键基础设施组织中的数百名专家对关键基础设施安全性的认识
- KIPS 获得了 SANS Institute 等领先教育机构的授权，可用于全球 SANS 学生的培训
- 安全服务提供商和供应商也授权在为关键基础设施客户提供培训时使用 KIPS，包括三菱日立电力系统株式会社
- KIPS 是欧盟委员会 Geiger 项目的一部分，旨在为小微企业提供安全培训和保护，帮助其抵御网络威胁并加强隐私管理

开设培训师培训课程

如果客户想使用 KIPS 对更广泛的受众（例如多个部门或工作地点的大批员工、管理人员和专家）进行培训，可以购买 KIPS 培训许可证，这样方便对内部培训师进行培训，并可以按照自己的时间和进度安排来开展 KIPS 培训。

这种类型的许可证包括：

- 在内部使用 KIPS 培训课程的权利。
- 一套培训材料以及使用/复制该材料的权利。
- 在许可证有效期内访问 KIPS 软件服务器的登录名/密码。
- 为项目负责人提供关于如何开展 KIPS 培训的培训师指导、教育和培训。
- 维护和支持（KIPS 软件和培训内容的更新与支持）。
- KIPS 场景的定制选项（需支付额外费用）。

面向合作伙伴和培训中心的 KIPS

KIPS 可提供绝佳机会，让合作伙伴通过各种方式从安全意识解决方案中获益。他们不仅可以将 KIPS 作为产品销售，比如出售给培训中心的客户，还可以用作内部培训（通过这种方式，卡巴斯基的培训专家可以提升合作伙伴的培训技能。）

Kaspersky Security Awareness

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。

卡巴斯基安全意识 – 掌握 IT 安全技能的全新方法

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。
游戏式学习体验调动了高层管理人员的兴趣，使他们成为网络安全计划的倡导者和建立网络安全行为文化的支持者。游戏化评估有助于找出员工的知识缺口，并激发他们进一步学习，而在线平台和模拟则帮助他们培养并加强相关技能。

持续学习周期

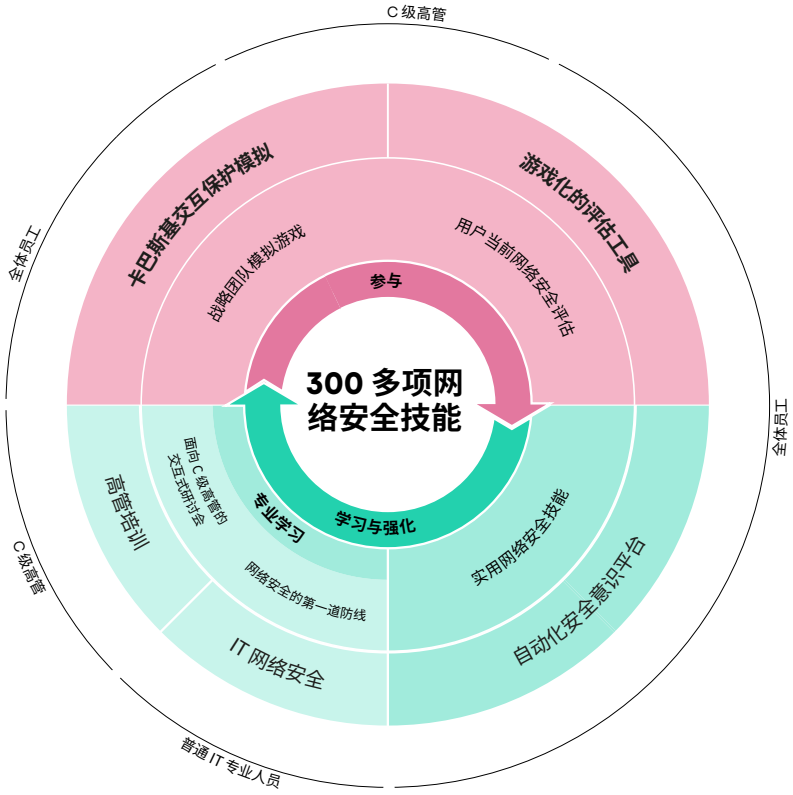
参与/动力
- 我为什么需要它？
- 认知

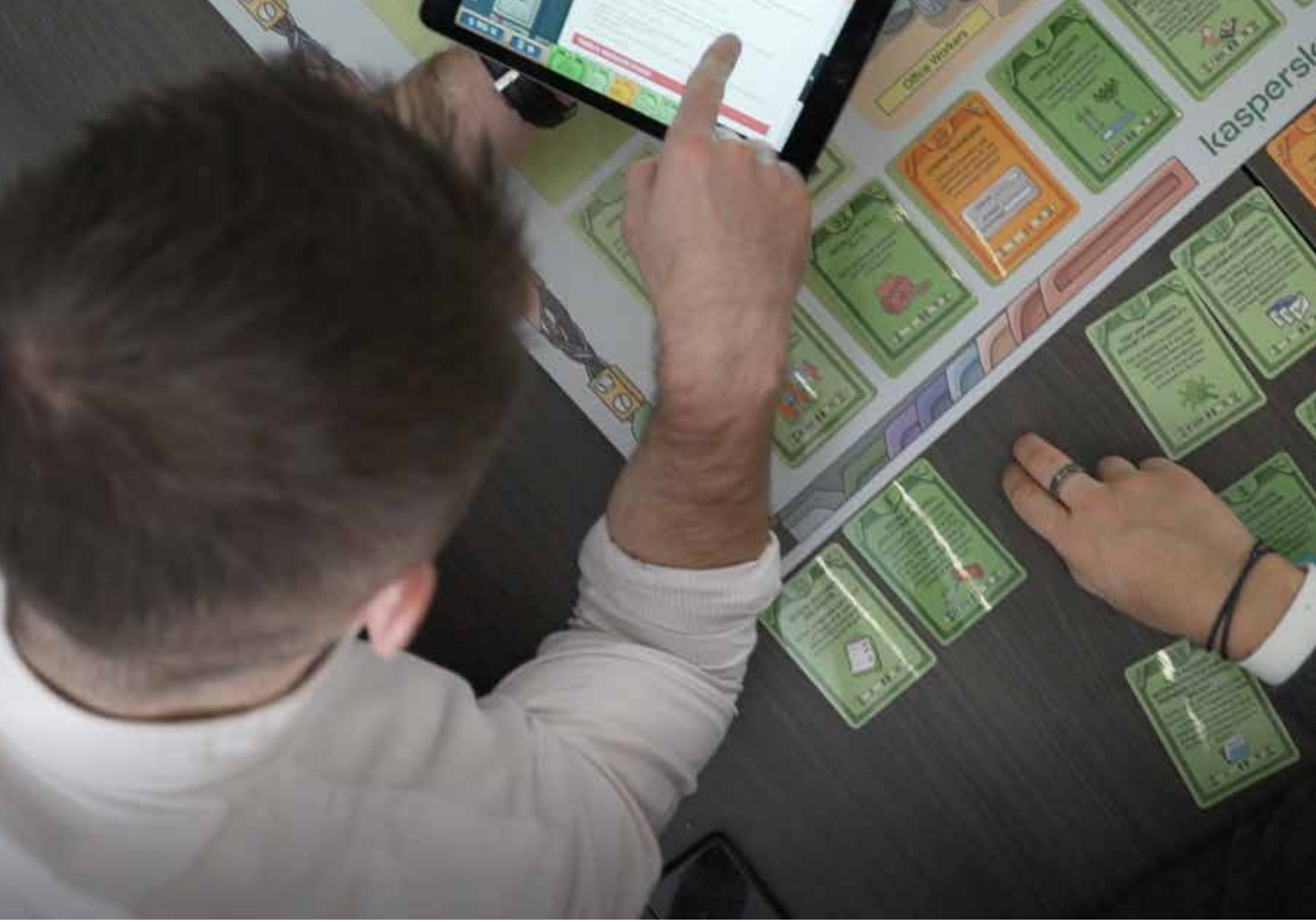
起点
- 我具备相关意识吗？
- 我都了解些什么，差距在哪里？

学习
- 微学习
- 持续学习
- 应变能力

强化
- 我做对了吗？
- 我还记得这件事吗？
- 我有相应地采取行动吗？

面向不同组织级别的不同培训形式





企业网络安全：www.kaspersky.com.cn/enterprise
卡巴斯基安全意识：www.kaspersky.com.cn/awareness

www.kaspersky.com.cn

kaspersky