针对一般 IT 专业人员的一线事件响应培训

IT 在线网络安全

免费试用
cito.kaspersky.com

kaspersky 引领未来

Kaspersky Cybersecurity for IT Online

IT 在线网络安全 (CITO)

交互式培训帮助普通 IT 专业人员培养强大的网络安全和一级事件响应技能

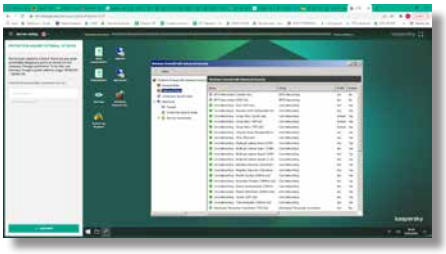
没有对所有相关员工的系统教育，就不可能创造出强大的企业网络安全态势。
大多数企业提供两个级别的网络安全教育和培训：为 IT 安全团队提供专家培训，为非 IT 员工提供安全意识培训。卡巴斯基提供了涵盖这两个级别的一套全面产品。还缺少什么？对于 IT 团队、服务台和其他技术先进的员工来说，只有标准意识培训计划是不够的。不过，他们不需要成为网络安全专家——这太昂贵且太耗时。

培训形式

培训完全在线上进行。学员只需要能上网和在个人电脑上有 Chrome 浏览器。共有 6 个模块，每个模块由简短的理论概述、实用技巧和 4 到 10 个练习组成，涵盖特定技能，教授学生如何在日常工作中使用 IT 安全工具和软件。

学习计划在一年内进行。建议的进展速度为每周练习 1 次，每次练习用时 5 到 45 分钟完成。

当前版本的培训针对 Windows 企业环境。



培训交付方式：
云或 SCORM 格式

一线事件响应

卡巴斯基正在面向通用企业 IT 专业人员推出市场上首个在线技能培训。它由 6 个模块组成*：

- 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 Security

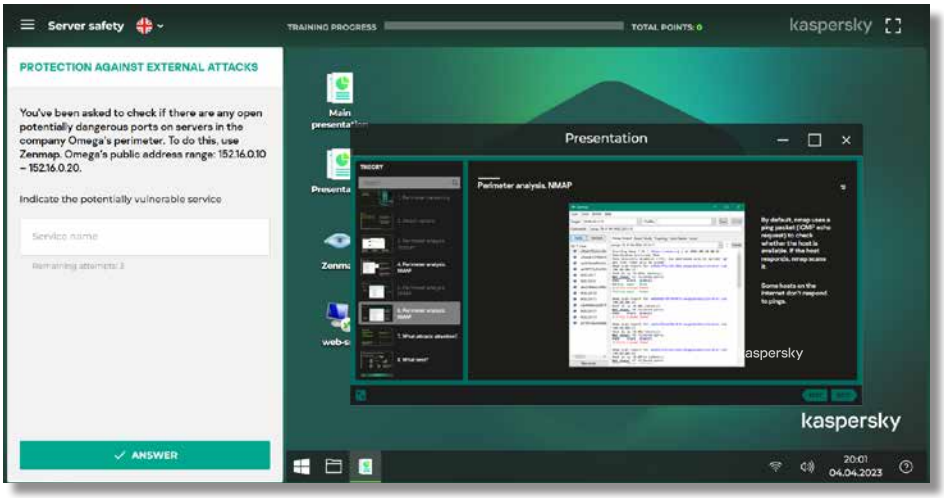
该课程为 IT 专业人员提供实用技能，教授如何识别看似无害的事件中可能隐藏的攻击情景，以及如何收集事件数据以移交给 IT 安全部门。它还能创造搜寻恶意活动迹象的激情，巩固所有 IT 团队成员作为第一道安全防线的角色。

为什么 CITO 培训有效？

- 交互式：模拟真实过程而不会对计算机有任何风险
- 创造技能和知识：从实践中学习
- 直观的学习过程：方便的导航和提示
- 涵盖了通用 IT 人员在工作中面临的所有主要 IT 安全主题和问题

学习过程

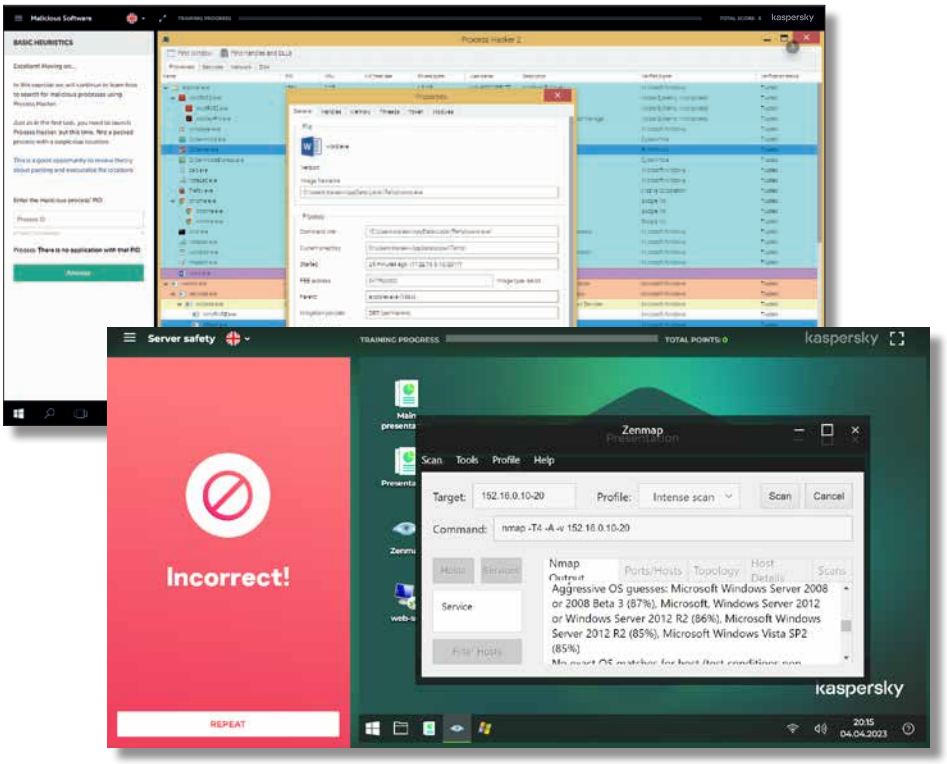
每个学习练习块由两部分组成：教育和实践，其学习任务均是模拟与先前解释相关的真实过程。



* 有关最新的主题列表，请查看 cito.kaspersky.com

当你上完课后，请完成任务

如果做得好，您将被引导到下一个练习块；如果做得不太好，您可以使用提示或重新阅读课程材料来更新知识

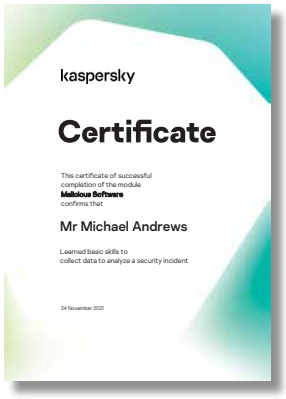


这个培训的对象是谁？

我们建议组织内的所有 IT 专业人员（特别是服务台和系统管理员）参加此培训。但是大多数非专家 IT 安全团队成员也能从本课程中受益。

证书

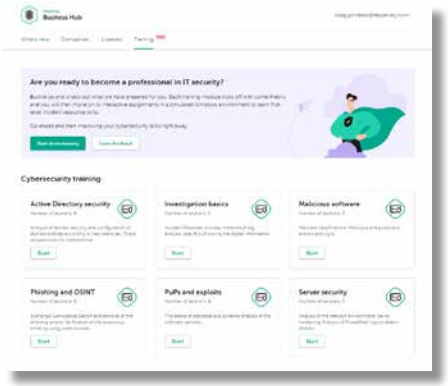
每个模块完成后，员工可获得个人证书



培训主题和成果

模块名称	目标受众	获取的知识	个人态度	所学技能	模块中给与的实践
恶意软件	对服务器和/或工作站具有管理权限的用户	恶意软件技术和分类 恶意软件和可疑软件的行为和迹象 启发式分析基础	恶意软件可以存在于计算机上的任何地方 恶意软件可以通过多种非同寻常的方式窃取数据 必须向安全团队报告所有可疑的潜在事件	验证是否存在恶意软件相关事件	使用 ProcessHacker, Autoruns, Fiddler, Gmer 工具检测恶意软件

模块名称	目标受众	获取的知识	个人态度	所学技能	模块中给与的实践
潜在有害的程序和文件 (PuPs)	有权安装附加软件的用户，以及可主动评估/打开从外部接收到的文件的用户	软件样本和可疑文档的统计与动态分析基础	文档（pdf，docx）可能包含漏洞 未签名的文件可能包含恶意软件或风险软件 所有未签名的可执行文件应该被检查是否可能有感染 数字签名不能保证文件不包含恶意功能	使用系统和沙箱事件监视器 使用统计引擎 移除 PuP	软件样本的静态（签名）和统计（virustotal）分析 使用 procmon 搜索软件的漏洞和恶意行为 使用 Cuckoo 沙箱进行文件分析 使用 AVZ 创建恶意软件删除脚本
调查基础	参与安全团队领导的取证或事件响应活动的 IT 员工	事件响应过程 日志分析方法 存储数字信息的具体情况	如果您怀疑有网络安全事件，请立即向安全团队报告并收集数字证据 分析应在安全团队的监督和合作下进行	收集数字证据 NetFlow 流量分析 时间线分析 事件日志分析	收集易失性和非易失性数据 (FTK-imager) 日志分析以查找攻击的来源和链接（eventlogexplorer） 利用 NetFlow 分析 (ntop) 进行横向移动调查 使用 Autopsy 进行磁盘分析
网络钓鱼和开源情报 (OSINT)	涉及取证或事件响应活动的 IT 员工	现代网络钓鱼方法 电子邮件头的分析方法	网络钓鱼可能非常复杂，难以发现，但总是可以通过手动调查检测到 钓鱼邮件需要从用户的邮箱中删除	钓鱼电子邮件分析和删除用户邮箱中的混淆钓鱼电子邮件 开源情报，用于了解黑客对您公司的了解程度	在 Exchange 邮箱中搜索和删除钓鱼电子邮件 使用 Recon-ng 进行网络侦察
服务器安全	服务器管理员	分析网络环境 服务器强化 分析 PowerShell 日志以检测攻击	网络边界漏洞是主要的攻击媒介之一。关闭所有漏洞不可能——您需要减少攻击面，尽量增加攻击者面临的困难。即使没有阻止入侵者，它也能为您争取时间进行检测。	搜索易受攻击和非标准的网络服务 根据"默认拒绝"原则配置系统 在 PowerShell 日志中搜索攻击迹象	使用 Nmap 查找易受攻击的网络服务 为程序控制配置软件限制策略，为网络控制配置 Windows 防火墙 使用事件日志资源管理器分析事件
Active Directory Security	Active Directory 管理员	使用 API 检查外泄密码数据库中的密码 根据建议配置域策略 分析活动目录域安全的方法	从安全角度来看，默认的 Active Directory 配置不是最佳。 攻击者可以通过多种方式提升其特权。 研究安全建议，使用为 Active Directory 提供更好可见性的工具	安全检查数据库中的密码哈希 搜索建议的域策略和实际域策略之间的不一致之处 评估 Active Directory 设置的安全性	使用 Have I Been Pwned?搜寻破解密码资料库的 API 使用策略分析器将当前域策略与最佳实践进行比较 使用 Ping Castle 报告



与卡巴斯基网络安全解决方案 - 云版集成

通过 CITO 培训提高您的网络安全技能，充分利用专业的网络安全产品。KES Cloud Pro 用户可直接从 Business Hub 获取该培训。

卡巴斯基安全意识 – 掌握 IT 安全技能的全新方法

培训计划的关键优势

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

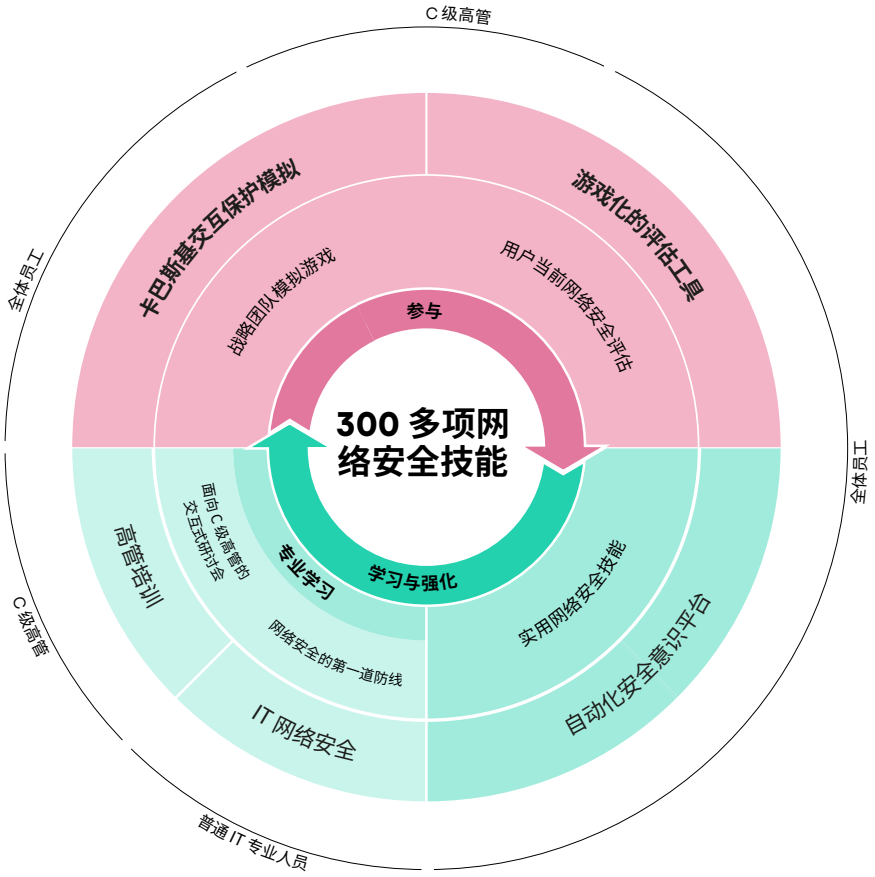
改变组织各级员工行为方式的培训
我们的游戏化培训采用寓教于乐的方式，吸引员工参与、激发员工动力，而学习平台则有助于吸收理解网络安全技能集，以确保员工不会边学边忘。

一个面向所有人、灵活的培训解决方案

“卡巴斯基安全意识”长期以来在国际上取得了一系列成功。它被各种规模的企业用来**培训超过 100 万名员工，覆盖超过 75 个国家**，它汇集了卡巴斯基超过 25 年的网络安全专业知识和在成人教育领域的丰富经验。

该产品组合提供了一系列吸引人的培训选择，在每个级别的员工中**提高网络安全意识**，赋能他们在组织的整体网络安全中发挥各自的作用。

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。基于游戏的学习可吸引高级管理人员，将他们转变为网络安全倡议的倡导者和建立网络安全行为文化的支持者。游戏化评估有助于确定员工知识的差距并激励他们进一步学习，而在线平台和模拟则为他们提供、加强合适的技能。



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

www.kaspersky.com.cn

kaspersky 引领未来