**安全竞赛服务**

**网络攻防竞赛**

|  |  |
| --- | --- |
| 网络安全知识理论竞赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |
| CTF解题赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |
| AWD攻防赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |
| 综合渗透赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |
| 应急响应赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |
| 车联网安全赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |
| 数据安全赛 | 根据行业需求、技术水平针对性定制培训、定制赛题、比赛平台、现场运维等,为客户提供一体化竞赛方案、对标国际高水平安全赛事,打造高水平竞赛。 |

网络攻防竞赛是一个为网络安全知识竞赛、技能竞赛等提供支持、服务的竞赛平台。它不仅为竞赛组织者提供便捷的竞赛组织、管理和统计分析工具，还为参赛选手提供公平的竞赛环境和丰富的竞赛内容。竞赛平台通过数字化手段，使得竞赛活动更加高效、透明和具有吸引力。

**网络安全实训**

|  |  |
| --- | --- |
| 培训课程 | 为学员提供海量培训课程，涵盖网络安全法规、Web安全、逆向分析等多个方向的课程体系，为用户提供全面的网络安全知识培训。 |
| 练习训练 | 提供理论基础和实操演练两部分训练。理论基础题覆盖移动安全、主机安全、网络安全、应用安全、数据库安全、云安全、密码学、法律法规、安全防护、安全运维等多方向网络安全理论知识，以单选题、多选题、判断题等方式呈现。实操演练提供在线、离线两种方式，满足不同场景需求。涵盖web安全、逆向工程、二进制漏洞挖掘与利用、密码学、杂项、真实漏洞等各个安全方向的题型，题量丰富，攻防兼备，为用户提供全方位的训练。 |
| 技能考核 | 通过考核可以检验学习成果，并配套评卷机制、成绩管理，全面掌握学员学习情况。 |

实训是集课程培训、练习训练、技能考核等功能于一体的网络安全实战培训系统。能够提供丰富的体系化训练内容，涵盖多方面的理论基础教学和实操演练，用于支撑网络空间攻防实战能力教学与培训，为用户提供全面的网络安全知识培训，提升网络空间攻防基础知识，培养网络空间攻防实战能力。并支持定制化的课程设置、考试模拟，满足不同人才培养需求。

**攻防演练**

|  |  |
| --- | --- |
| 实战化攻防演练 | 在攻防演练前，平台能够对内部资产进行盘点和风险分析，评估外部暴露面和抗攻击能力，帮助用户识别潜在的安全风险。在演练过程中，平台提供多维检测和关联分析功能，实时监控攻防流量，自动响应阻断攻击，并深入业务应用监测，精准定位业务安全问题。演练结束后，平台能自动生成安全态势报告，帮助用户进行策略优化和知识沉淀，提升整体安全防御能力。 |
| 安全防护与监测 | 提供高级持续性威胁预警、文件威胁分析和网络流量审计等功能，帮助用户实时监测攻击、自动响应阻断，并深度分析溯源。集合网站域名安全防护、Web攻击防护、DDoS攻击防护等多种安全功能于一体，为网站提供一站式的安全防护。利用欺骗防御理念构建蜜罐环境，引诱攻击者偏离真实目标，在伪装环境中监视入侵行为，自动溯源攻击者身份，甚至进行深入反制。 |
| 运维保障与技术支持 | 依托丰富的攻防演练组织经验，平台提供成熟的演习计划和应急方案，确保用户能够安全无忧地进行运维。平台拥有大量经验丰富的网络安全攻防专家，不仅能够参与靶场技术研发工作，还可作为实战攻击队或专家裁判参与演习。提供包括风险面识别与收敛、系统安全评估与加固、安全策略优化、靶标加固、模拟攻防演练、应急演练等在内的全方位服务。 |
| 攻防可视化与追溯 | 通过指挥调度、攻防态势等可视化功能，直观展示攻守双方的实时战况、攻防成果以及现场情况。所有终端数据、流量数据、现场视频数据等均被留存，确保演练过程的可追溯性，为后续的安全分析和改进提供依据。 |

网络安全攻防演练是一款承载网络攻防演习活动的支撑平台。它以真实生产环境为战场，以攻防对抗的形式进行实战演习，对系统安全防护能力、安全运维能力以及安全事件的监测和响应能力进行全面的检验。平台对攻击团队的攻击过程实现全面监控，从攻击终端、网络通道、数据分析等多个环节充分保障演习的安全性、可靠性、时效性和灵活性。最后通过平台对演练过程和结果进行数据分析和可视化展示，直观地反映出攻守双方的实时战况、攻防成果以及攻守双方现场情况，有利于直面网络安全问题,摸底网络安全现状，进一步加强网络安全应急管理，提升网络安全事件应急处置协作能力，积极应对突发网络安全事件的实战经验。

**钓鱼演练**

|  |  |
| --- | --- |
| 钓鱼演练服务 | 通过模拟黑客邮件钓鱼的攻击方式，对企业人员开展实战化钓鱼演练。明确需求、演练对象、演练时间等，开展实战化演练，并统计汇总演练结果。采用高仿真实时渲染技术，实现对静态网页的1:1仿真克隆，支持交互操作确认页面关键信息输入位置，达到目标站点隐私信息获取目的。 |
| 网络钓鱼防范培训 | 根据演练效果对客户相关人员开展网络钓鱼防范培训。针对易中招邮件特点和邮件攻击中的脆弱点，进行有针对性的培训。 |
| 超仿真邮件钓鱼 | 以超仿真邮件攻击为核心理念，从攻击者视角出发，模拟整个邮件攻击过程。支持钓鱼网站容器化部署，与平台部署分离，支持在多个机房部署钓鱼网站。 |
| 数据采集与脱敏处理 | 钓鱼网站采集到的账号、密码等敏感信息，存储在Docker内，用户可进行脱敏处理，避免敏感信息的泄露。 |
| 可视化展示与数据分析 | 收集企业成员在钓鱼演练中的操作行为数据，可视化展示企业中高风险部门，帮助企业发现脆弱点。输出演练总结报告，提供详细的数据分析和改进建议。 |

钓鱼演练是一种专门设计用于模拟和训练防御网络钓鱼攻击的产品。该平台旨在帮助组织和企业提高员工对钓鱼攻击的识别能力，以减少安全漏洞和数据泄露的风险。其通过模拟黑客邮件钓鱼的攻击手段，以“黑衣人”身份通过平台向企业指定用户邮箱发送钓鱼邮件，并对被钓鱼成功的安全意识薄弱职工进行风险预警提示。配合企业总部或安全部门完成对人员安全意识的垂直检查工作。