

大话赛宁云 | 演系列-超仿真网络空间“演武场”

原创

Cyberpeace 于 2022-01-28 14:22:51 发布 4114 收藏

文章标签: [网络](#) [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Cyberpeace/article/details/122730781>

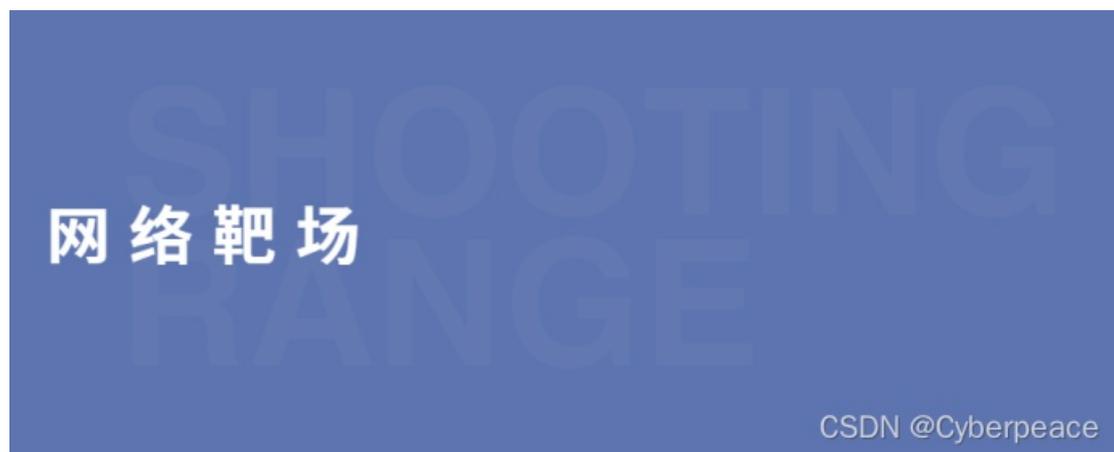
版权

近年来, 随着国际网络安全事件的频发, 网络安全防御也逐步得到人们的广泛关注。各行各业开始实施HW行动, 因此, 通过构建网络靶场, 培养网络安全的攻防能力是当前信息化时代极为重要的发展方向。

解决网络安全问题, 需要首先在虚拟空间培养实战能力, 就是在网络环境中, 通过仿真技术, 在靶场上进行对抗演练, 渗透防护等一系列的战术推演, 提升人员的安全技能和综合防护能力, 方可在实战中进行运用。

一个超仿真演练平台

针对网络安全危机, 赛宁网安全全面建设靶场实现HW行动, 为国家乃至国际各行业提供更有价值的靶场演练空间。赛宁云一云六系“演”系列, 推出多元化、超逼真的演练平台。平台主要功能有: 环境孪生、3D态势、指挥调度、复盘推演、攻防作战、战术推演、裁定评判。其包含的产品众多: 网络靶场、工控靶场、物联网靶场、密码靶场、活体漏洞靶场、电磁对抗靶场、无线通信靶场、卫星靶场、电力/能源/交通靶场、城市级-数字孪生靶场都应用于国家各个领域和关基础设施之中。



“演”系列拥有强大的产品综合优势

- 1、核心技术源于清华大学蓝莲花战队，实战能力亚洲第一、全球第二；
- 2、同时出口全球十几个国家，成为一带一路国家重要的安全基础设施；
- 3、超复杂异构网络、支持10万+节点高并发、100万+IOT设备灵活接入；
- 4、提供1万+靶标、无缝对接所有主流厂商安全设备；
- 5、支持虚拟化西门子、施耐德等多款主流PLC；支持工控设备、工控网络设备、工控安全设备等接入。

工控靶场

随着工控时代的到来，工控系统面临挑战，为提升工控系统网络安全能力，基于赛宁云“演”系列推出工控系统网络安全靶场。赛宁网安深入研究工控网络结构和特征，全层级还原工控系统。通过模拟攻击行为和防御措施，展现攻击效果、验证防护措施的有效性，帮助工业企业升级综合防护能力、提升人员安全意识和技能。覆盖能源、电力、石油、煤炭、交通、智能制造、通信等，具备全球多行业交付经验。



演系列案例

国内

重庆市合川区网络安全基地

赛宁网安在重庆合川区建设网络靶场，用于网络安全人才培养、网络对抗演练、系统测试和装备测试，致力于提高企事业单位的网络安全防护和对抗能力，同时带动重庆市网络安全产业发展，为产业、社会培养和储备大量网络安全专业人才，提升重庆在网络安全和新技术领域的创新能力。

“强网”拟态防御国际精英挑战赛

赛宁网络靶场作为测试床，提供了强大的网络虚拟能力和虚实结合能力，接入了数十款拟态设备用于黑盒测试和白盒测试，并通过全维事件采集接口，对攻击测试所产生的事件以及攻击流量等数据进行采集，成功验证了拟态防御理论的安全可行，为网络安全行业理论发展和技术应用起到巨大推动作用。

中国移动-网络安全运维演练

赛宁网安为中国移动网络安全运维演练进行保障支撑，结合中国移动通信集团实际，对典型信息系统、真实威胁（如DDOS、数据窃取等）进行超逼真模拟，开展超大规模的安全运维与应急响应演练。

国际

北非国家-网络靶场系统

赛宁网安具备国际影响力，与北非国家建立合作关系。赛宁网络靶场，为其提供了网络空间环境仿真、技战法研究、异构专业系统的测试、网络安全技能体系化建设，打造一支高技术水平的专业队伍，助力用户构建网络安全能力，接轨世界先进水平。

助力网络安全

一云六系-演系列凭借超逼真IT网络环境仿真技术，通过大规模渗透演练、情景式防护演练、高烈度红蓝对抗演习，提升关键信息基础设施企业的团队作战和战术推演能力。基于数字孪生靶场，通过网络靶场技术的创新，网络安全演练的推演，深耕网络靶场，大幅提升团队整体实战策略运用能力，建设成为网络空间的“演武场”。