Cisco Cyber Range 服务

概述

由于网络安全威胁已变得更加复杂、更具针对性和持久性，这给企业带来了一个严重、持续的挑战。仅有安全硬件和软件产品不足以阻挡目前最先进的攻击。现代网络防御要求由训练有素的人员主动采取安全措施，这些人员应当具备检测和瓦解复杂威胁的经验与专业知识。具备适当技能和经验的人员供不应求。

Cisco® Cyber Range 服务能够帮助安全人员获得应对现代网络威胁所需的技能和经验。根据实际情况，Cyber Range 提供一个虚构的对战模拟环境，可让安全人员扮演攻击者和防御者的角色，从而了解最新的安全漏洞破解方法以及如何利用高级工具和技术来缓解和根除威胁。

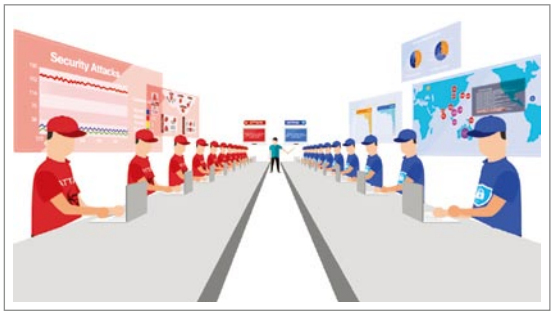
Cisco Cyber Range 服务提供：

- 应对和防范简单及复杂网络攻击的实际经验，包括高级持久威胁 (APT)
- 领先的安全方法、运维和程序方面的更深入知识
- 部署行之有效的检测模式以及利用最新安全工具和技术方面的高级技能
- 建立团队协作和责任管理，从而平衡工作负荷，将工作重点放在核心任务上

解决方案亮点

Cyber Range 是实际体验智能网络安全的一个平台。以飞行模拟器为例，飞行员可以在上面学习如何在不同飞行情况下操纵复杂的系统。对安全人员来说，Cyber Range 是一个类似的环境。Cisco Cyber Range 是一种模拟典型企业客户的网络和应用的沙坑环境。但是，该解决方案不仅重视技术，同时也兼顾人、技能、流程、数据以及连接到互联网的万事万物。

Cisco Cyber Range 服务基于以下组件构建：



- 基于运维主导的模式，汇集人、流程和技术的力量来应对网络威胁
- 在思科云智能安全服务的助力下，利用着重于威胁、可见性驱动和基于平台的工具
- 模拟 50 多种不同的攻击情形和 100 多种实际应用
- 不断更新最新的攻击和威胁情形
- 使用能在全球任何地方远程访问的虚拟环境

特性与优点

Cisco Cyber Range 服务模拟复杂的网络、服务器和应用基础架构环境。图 1 概要显示了 Cyber Range 环境。

应用与网络基础架构区代表典型的内部 IT 环境，模拟了互联网边界网关（网关块）、数据中心与应用服务（服务器块）以及本地与远程用户访问基础架构（用户块）。防御区代表安全运维中心。在防御区内，蓝色团队的成员可以访问一系列系统，以监控、应对和防范针对内部环境的威胁。攻击区代表外部环境。红色团队可以利用最新的工具和技术来攻击内部环境，包括通过网关块和从用户块攻击。监控区允许绿色团队（包括思科人员）控制和评估总体对战模拟。

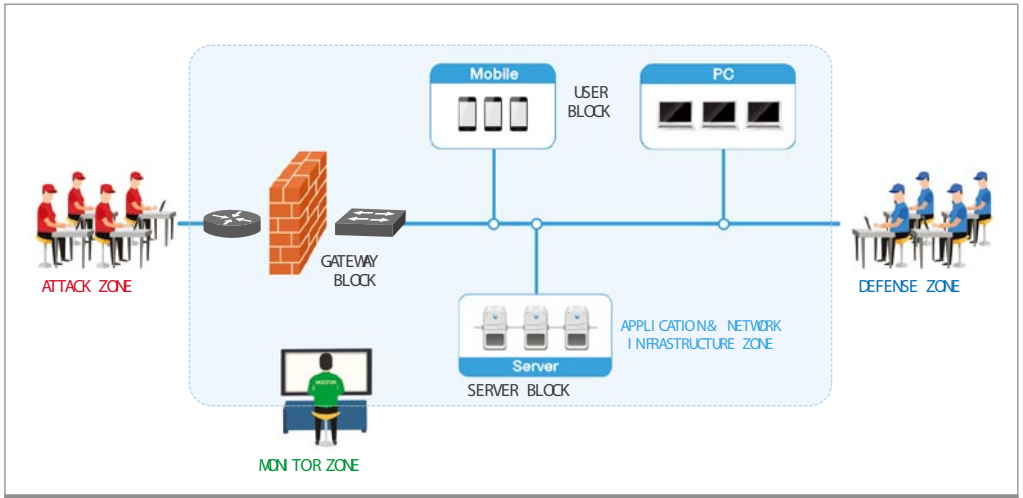


图 1 Cisco Cyber Range 环境

服务规格

Cyber Range 能够模拟众多的基础架构服务以及攻击和防御功能。表 1 列出了标准服务。

表 1：服务功能

基础架构	攻击	防御
• 有线、无线和远程接入 • 网络与路由 • 客户端模拟器 • 服务器模拟器 • 应用模拟器 • 流量生成	• 分布式拒绝服务 (DDoS) • 零天攻击 • 网络侦测 • 应用攻击 • 数据丢失 • 计算机恶意软件 • 移动设备恶意软件 • 越狱方法 • Botnet 模拟 • 开源攻击工具 • 虚拟网络攻击	• 全局威胁智能 • 客户端端点安全性 • 防火墙、IDS/IPS • 基于签名和基于行为的检测 • Web 和电子邮件代理 • 无线安全性 • 应用可见性与控制 • 遥测数据分析 • 身份与权限管理 • 安全与事件管理 • 调查工具 • 开源防御工具 • Cisco TrustSec® • 软件定义的网络

为什么要选择思科服务

Cisco Cyber Range 环境基于思科在客户环境中实施和运行安全性的多年经验，以及思科用于内部安全运维的工具和方法。Cyber Range 能够以许多重要方式模拟众多的基础架构服务以及攻击和防御功能。

- 架构设计验证
- 攻略创建和验证
- SOC 团队网络对战模拟练习和事件响应实践
- 某些技术的实操培训
- 威胁缓解流程验证
- 模拟新威胁（零天）或正在演变的威胁，以开发适当的缓解策略和方法

更多信息

要详细了解 Cisco Cyber Range 服务，请与当地的客户代表联系或发送电子邮件至 cybersecurity-apjc@cisco.com