产品资料

Cyber Exposure 研讨会

服务概述

Cyber Exposure 研讨会旨在评估现有的漏洞管理计划，并制定规划以优化 Tenable® 解决方案，最大限度缩小 Cyber Exposure 缺口，并降低业务受到的网络安全风险。

借助 Tenable 专业服务提供的 Cyber Exposure 研讨会，我们的行业专家将确保企业漏洞管理计划充分发挥作用。我们将与企业合作，确定计划目标，并了解 Cyber Exposure。服务结束后，企业将获得专为满足安全和业务目标而设计的漏洞管理计划定制路线图和运营计划。

Cyber Exposure 研讨会服务非常适合更庞大更复杂的环境，即符合以下情况之一：

- 已选择 Tenable 作为首选解决方案，但又希望了解具体的推行方式或最大限度降低推行风险。
- 尚未部署 Tenable 解决方案，希望就怎么做才能获得最佳效果听取专家建议。
- 已部署 Tenable 解决方案，但又希望从外部专家角度审查整体漏洞管理计划。

携手合作

Tenable 专业服务团队和我们的全球认证合作伙伴网络不仅仅限于基本安装服务，更能在部署前、部署中和部署后与各种规模的企业携手合作，致力于取得成功。Tenable 值得信赖的安全专家能够提供产品优化和行业最佳实践建议。他们多年来服务于全球数千客户并已从中积累了丰富的实践经验。在企业部署中充分利用 Tenable 专业服务，提升企业安全实践的成效，并为有效的基于风险的漏洞管理决策提供数据支持。

关键成果

- 在 Tenable 资深顾问和深厚的行业见解的帮助下，确保企业漏洞管理计划采用基于风险的方法
- 加快 Tenable 基于风险的漏洞管理专业能力的价值实现
- 通过实践经验和知识传授，全面掌握行业领先的理念
- 对运营和攻击面的状态获得深入了解和态势感知

Cyber Exposure 研讨会的步骤

活动 1：
规划、评估和制作评估报告

安全目标

- 探索内外部安全驱动因素
- 讨论网络安全趋势
- 审查当前的安全态势
- 明确期望的状态，包括安全目标

成果

- 了解 IT 战略、当前和期望的安全态势
- 确定要实现基于风险的漏洞管理旅程目标所需的高级别步骤

合规性要求

- 探索合规性要求

成果：

- 了解 Tenable 解决方案如何支持合规性需求

网络分析

- 从高层次了解网络拓扑、资产类型和可见性

成果：

- 确定关键资产类别和扫描优先级

评估运营能力

- 审查运营能力，包括：
- 漏洞评估，包括扫描、资产发现、分析、工单和补丁
- 配置标准
- 扫描类型和频率，包括发现、临时、自动、漏洞和合规性

成果：

- 与关键运营能力保持一致，支持运营计划的发展
- 利用 Tenable 解决方案能力，识别并弥补当前状态和期望状态之间的缺口
- 制定高层次的运营计划

活动 2：
解决方案审查、共享最佳实践和实施建议

工作流和自动化要求

- 了解实现安全目标所需的业务流程
- 尽最大可能识别并减少手动步骤

成果：

- 确认要管理的工作流步骤、数据要求和系统

报告要求

- 了解面向不同利益相关者的报告和可视化要求、期望的视图、内容、频率等

成果：

- 确认报告要求，包括报告的信息和报告的频率

解决方案设计和架构

- 检查并清点现有技术资产，以便：
- 使 Tenable 解决方案与风险优先级保持一致
- 确定能够满足业务目标的最佳分阶段部署方案

成果：

- 创建专为基础设施打造的的架构设计（包括 Tenable 和第三方产品）
- 提供具有可操作性的技术部署路线图

+ 识别未来的专业服务需求

企业会随着时间的推移而变化和发展。Tenable 专业服务有助于确保企业解决方案与不断发展的业务需求保持一致。

欲了解更多信息：敬请访问 tenable.com/services
联系我们：请发送电子邮件至 sales@tenable.com 或访问 tenable.com/contact