MANDIANT®

数据表

网络安全计划评估

评估您的网络安全计划，以优化投资、提高弹性和减少风险。

优势

- 识别和减少您环境中的网络安全风险
- 优先考虑网络安全投资和资源，以满足您的业务目标
- 了解现有安全控制措施的效能
- 提高高管层对网络安全挑战、计划差距和相关违规影响的认识

为何选择 MANDIANT 服务

自 2004 年起，Mandiant 始终走在网络安全防护和网络威胁情报领域的前列。我们的事件响应产品不断用于处置全球最复杂的违规事件。我们可深入了解原有和新兴威胁制造者，及其快速多变的策略、技术及程序。

概要

Mandiant 安全计划评估针对以下四个核心关键领域，对您组织的网络安全计划进行独立的成熟度评估：安全治理、安全架构、网络安全防御和安全风险管理。

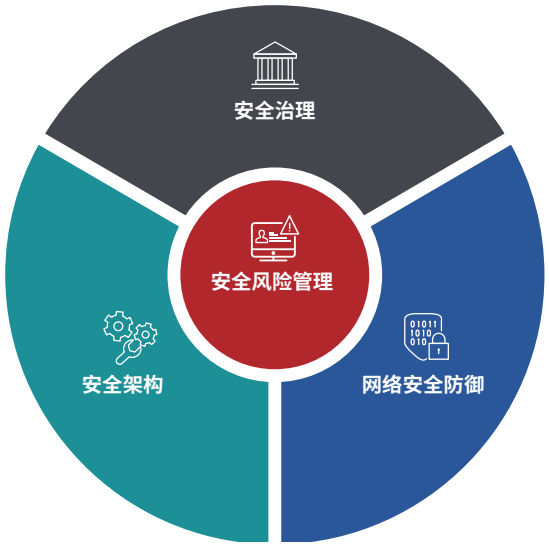
在对您现有计划进行深入的协作分析后，我们根据您的特定风险状况和安全成熟度级别，提供最佳操作建议，以改进您的安全态势。

我们的方法

Mandiant 专家对您组织的四个核心安全计划领域进行了深入评估（图 1）。他们基于我们积累的一线专长，采用专门构建的方法，满足主要的行业标准与框架。

图 1.

评估了四个核心安全域。



我们的专家首先审核您现有的安全计划功能和操作文档。他们同时收集相关行业部门的威胁情报，以及影响您特定环境业务部分的关键数据。初始分析阶段后，Mandiant 专家主持了一系列互动研讨会，以了解您组织当前的网络安全成熟度，并设计高效的未来计划模型，以满足您的业务需求。

我们的研讨会涵盖四个核心安全领域的新兴主题，如云安全基础结构、应用程序安全、供应链安全管理和威胁情报。

接下来，我们的专家会提交一份详细的调查结果报告，并提供战略和战术改进建议。我们的专家还将为您提供多年实施路线图，以满足您组织的短期和长期网络安全目标。

为确保长期的成功和可持续发展，我们的专家还可以：

- 使用 Mandiant Security Validation（安全验证）平台针对路线图行动实施进行安全效能评估
- 执行 Mandiant红队判研 (Red Team)评估和 Mandiant Penetration Testing（渗透测试），以确保采用最佳的检测和响应功能
- 执行其他安全架构和配置审核，以改进或增强防御功能。

Mandiant 致力于使该服务带来最高级别的保真度，支持您的组织从设计阶段到实现运营效率。

图 2.

服务工作流程和活动时间表。

第 1 步	第 2 步	第 3 步	第 4 步
文档收集、审核和分析	互动研讨会和行政会议	报告和建议开发	质量保证和报告交付
1 周	**2 周**	**2 周**	**1 周**

活动成果

- **执行摘要：**关于您组织的计划成熟度、优势领域、改进机会及实施路线图的高级概述。
- **评估结果和未来状态目标：**识别需要进一步开发的关键安全功能域，以及有针对性的未来状态成熟度模型。
- **可操作路线图：**含优先级建议的战略和战术计划，可帮助增强组织在所有四个核心安全领域的安全成熟度。
- **行业部门威胁情报：**通过对可操作威胁情报的广泛事件响应经验，深入了解影响您行业的全球攻击者行为。
- **执行和技术简报：**向高层和技术利益相关者演示评估结果。

若要了解更多信息，请访问 **www.FireEye.com/mandiant**

FireEye, Inc.
中国上海市黄浦区淮海路东段淮海中路 99 号大上海时代广场 26 楼 China
china@fireeye.com

M-EXT-DS-US-EN-000006-06

关于 Mandiant Solutions
Mandiant Solutions 将全球领先的威胁情报、一线事件响应数据、持续的安全性验证结合，为组织提供了所需工具，以提高安全性和降低业务风险。

MANDIANT®