MANDIANT®

安全防御能力验证

证明网络安全的价值

首席信息安全官 (CISO) 必须证明安全有效性

如今的风险感知商业环境为首席信息安全官及其团队带来了压力，要求他们保护企业资产，保护组织的财务状况和品牌价值。他们必须向管理层证明网络安全投资的价值，以及在有效防止对手破坏关键系统的有效性。

但是由于缺少验证安全、量化风险、展示运营能力所需的工具，他们依靠漏洞扫描程序、渗透测试、红色团队或违规和攻击模拟功能。由于固有的局限性，这些方法未充分评估有效性，也未能及时对组织面临的特定、高度优先的威胁提供相关、及时的见解。

此解决方案为 Mandiant Security Validation（安全防御能力验证），其为持续、智能化产品组合，由独特的性能模块和 Mandiant 安全检测平台组成。[1]

证明有效性并量化您的网络安全计划

安全防御能力验证的执行基于五步方法，提供关于最重要测试元素的见解，以及如何根据目标组织或行业优化防御。

图 1. Mandiant 五步以情报主导防御能力验证方法。

1 前 Verodin 安全检测平台 (SIP)。

此方法要求可实时利用威胁数据。Mandiant Security Validation 使用 Mandiant 威胁情报和事件响应数据，以无与伦比的对比可见性，反映攻击者的行为。安全团队根据情报安全防御能力验证，识别其组织面临的高优先级威胁，基于组织威胁创造者和实际威胁创造验证策略。安全负责人及其团队通过 Mandiant 对所有技术、流程和人员执行全面、持续的安全控制验证。

Mandiant Security Validation 采用安全检测平台及其控制验证技术帮助安全团队对真正的攻击行为进行安全控制，以快速量化和证明安全计划的有效性，并可低于最复杂的对手攻击。

Mandiant 安全检测平台的基本功能：

- 优先考虑最重要的威胁和对手控制措施
- 评估真正对手攻击的安全控制有效性
- 通过无与伦比的 Mandiant 威胁情报和事件响应数据，安全执行相关攻击
- 发现组织安全基础架构中未检测到的漏洞
- 识别最佳优化机会
- 量化评估随时间的防御情况
- 通过可量化的证据，实现高管投资的合理价值

Mandiant 安全检测平台配备高级功能：

- **威胁参与者保证模块：**使威胁情报可操作，以测试对真正威胁参与者的控制情况，特别是对有可能针对组织发动攻击者。TAAM 与第三方行业领先的情报源集成。
- **高级环境偏移分析：**支持对 IT 基础架构的持续监控，消除环境偏移，对防御性环境进行持续验证，确保组织安全基础架构正常运行。
- **受保护威胁者：**通过安全执行恶意软件、勒索软件和其他破坏性攻击验证端点控制有效性，以主动保护最新和新兴的威胁。
- **电子邮件威胁者：**测试电子邮件安全平台中提供的控件。

Mandiant Security Validation 产品组合包含多种部署选项：

- **客户拥有：**基于云（安全即服务（SaaS）），或在本地部署为虚拟设备。
- **全面托管和共同管理的模型：**根据客户所需的业务效果，Mandiant 团队创建计划以契合特定用例，持续向客户利益相关者提供详细报告。
- **按需防御能力验证：**使客户能够购买单个用例，从而一次性评估其能力，阻止预定义攻击或威胁参与者，获得关于进一步调查所需建议，改善防御，降低风险危险性。

图 2.

此平台有助于查看和生成“您的控制措施正在保护关键资产”的证明。

安全防御能力验证为企业带来的优点

评估有效性和投资收益 (ROI)

获取可量化数据，帮助确定必要投资，以提高针对优先攻击类型的安全有效性，并量化您的总体风险状况。安全团队还可利用此证据，通过执行领导和董事会，实现合理的安全投资价值。

并购

清楚地了解公司在并购时可能出现的控制重叠或差距。您可通过合理支出，计算整合所需的潜在金额，以及合并可能造成的风险水平。

招募和培训安全人才

了解其过去的经验，并评估安全专业人员的学习潜力、拥有的经验类型，以及他们的技能组合在真实场景中与组织环境的匹配情况。通过在整个生产环境中安全地执行攻击，IT 领导者可以监控潜在候选人的应对和反应情况。IT 负责人还可以定期执行培训练习评估，以查看团队在实际攻击情景中是否表现出可接受的响应时间和所需的技能。

品牌保护

主动、持续地衡量安全有效性，以降低违规或攻击的风险，维护您的品牌声誉和客户忠诚度。

数据隐私和保护

保护客户数据并确保遵守法规、公司和第三方授权规定。

以 Mandiant 威胁情报为基础的安全验证

在最近 15 年多的时间，Mandiant 通过在全球调查、事件咨询和标红团队措施，创建并策划了独特的威胁情报组合，不断更新证据数据、人类专长和独特的分析情报技术。Mandiant 现在通过以下平衡来源集合，主导网络威胁情报领域：

- **泄漏情报**的收集方式为 Mandiant Consulting 事件响应活动
- **对抗性情报**由 Mandiant 研究人员获取
- **机器情报**来自 FireEye 安全产品
- **运营情报**源自 Mandiant Managed Defense 服务

欲进一步了解 Mandiant Solutions，请访问：**www.FireEye.com/validation**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

关于 Mandiant Solutions

Mandiant Solutions 将全球领先的威胁情报、前线事件响应数据、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。

©2020 FireEye, Inc. 保留所有权利。
FireEye 和 Mandiant 是 FireEye, Inc.的注册商标。其他所有品牌、产品或服务名称是或可能是各个所有者的商标或服务标记。
M-EXT-DS-US-EN-000317-01