MANDIANT®

数据表

Security Instrumentation Platform 安全检测平台

了解真正的安全措施

亮点

- **根据及时和相关的网络威胁情报**优先排序这些威胁
- **评估当前安全工具应对**真正对手攻击的效率
- **发现安全基础架构中的未检测差距**和重叠项
- **评估您团队的**检测和响应时间
- **识别最佳**优化机会
- **随时间推移的**防御量化改进
- **通过可量化的证据，**实现高管投资的合理价值
- **简化整个企业**对安全态势的沟通

如今环境中的动态威胁日益增加，首席信息安全官及其团队在应对挑战，保护公司资产安全。他们应了解并提供证据，证明他们的网络安全投资的价值，以及网络防御对当前和正在出现的对手攻击的有效性。

渗透测试、红队研判、泄漏模拟和攻击模拟远远不够—他们无法为首席信息安全官和企业负责人提供必要的可量化证明，因而无法了解风险危险性和网络准备情况。如无基于性能数据的证据，则安全团队无法成功优化防御和自信报告其安全态势。

Mandiant 安全检测平台（Security Instrumentation Platform）是 Mandiant 情报控制验证技术的关键组成部分，可提供您需要的证据。此安全检测平台为网络安全风险评估和管理平台，可帮助团队始终保护其安全资产。

改进控制效率

Mandiant 安全检测平台基于 Mandiant 全球威胁情报和事件响应数据，其为独特且无与伦比的威胁数据，可实施了解攻击对手的攻击行为。Mandiant 威胁情报和安全验证技术的结合，根据组织的攻击者和攻击内容信息，验证其策略。

Mandiant 情报主导的安全验证技术优先安排关键、相关的威胁，然后安全地评估和捕获分散的量化证据，证明您的整体安全架构对真正对手攻击的有效性。此结果突出显示了特定的个体攻击，甚至可击败或绕过您安全技术的整个击杀链延伸区域。您可使用此信息，按需使用指定数据，并与供应商合作，确定控制措施优化的位置和方式，并最终转变您的整个计划。

您可通过 Mandiant 的安全检测平台，快速量化和证明您的安全计划在对抗世界各地最新的复杂对手时的有效性。此计数可通过本地、云端和混合基础架构使用。

量化您的效率提高情况，可证明您的安全调查对公司企业负责人的风险承受能力的价值。

通过 Mandiant 安全检测平台，此流程可实现自动化和连续性，让您能够更战略性地专注于保护您的业务，同时平台可密切监控和衡量您的整体安全有效性。

获得对安全态势的信心

Mandiant 安全验证专家可与您合作，快速配置平台、联系参与者、提醒来源见及任何指定控制措施，以获取更深入信息。通过易于集成的特点，当安全执行攻击行为时，您可查看防御堆栈的表现。

配置后，您可从 Mandiant 的大量真实攻击库、对手技巧、战术、程序和各类恶意软件中选择离散测试或预配置序列。随着这些测试的安全运行，您可即时和持续验证指定控制措施是否适当。随着测试的运行，控制面板会实时填充，以向您展示检测、提醒、缺失和预防的速率。

该平台还验证事件是否采用正确的时间戳和经过正确分析，如果定义了相关规则和威胁模型，则事件将生成相应的警报。概述您一段时间的整体安全有效性的报告可供查看和导出。通过连续、持续的验证，您可获得一定的证明，以实现并保持您对计划的信心，不仅仅是您自己，还有您的高管和董事会。

平台细节

Mandiant 的开放、可自定义和可扩展平台提供了自动控制发现和基础架构，允许通过真实攻击二进制文件安全地测试安全控制措施。其包含 6 个核心要素。

控制器

此中央控制器和管理器提供动态生产环境的持续验证，可用基于云的（安全即服务）平台或本地虚拟设备或可安装软件。

参与者

他们在生产环境中安全执行测试，以验证网络、Windows、MacOS 和 Linux 终端、电子邮件和云安全控件的有效性，确保您的基础架构适当配置。

集成

与防御技术和安全基础架构进行丰富、开箱即用的集成，可完成更深入的控制验证。

攻击库

此内容库所示为对手周期每个阶段的上千次攻击，包括延长杀伤链，以及基于 Mandiant 全球威胁、对手和泄漏情报的当前和新型击杀链攻击行为和 TTP。

框架

攻击可与 MITRE™ ATT&CK 和 NIST 框架保持一致，以轻松将有效性融入您的安全评估计划。Mandiant Security Validation 的独特之处在于，其内容为攻击框架战术与组织关联情况的见解，其可用于运行 MITRE ATT&CK 战术，确保全面、相关的测试和准确的结果。

控制面板和报告

实时图形显示，其中包含在您的环境中运行的测试结果，以及一段时间有效性改进的报告，其中包含可用于通知您的高管的真实定量数据（图 1）。

图 1. 控制面板有助于在整个攻击生命周期内验证安全控制措施，以查明风险区域。

情报验证技术

Mandiant 安全检测平台通过自动化环境偏移检测，对安全控制措施执行全面、持续的监控、验证和优化。此持续验证流程通过五步骤情报方法执行（图 2）

图 2. Mandiant 五步情报验证方法。

高级功能

- **威胁参与者保证模块 (TAAM)：**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（图 3）。
- **自动环境变化/偏移分析 (AEDA)：**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终端控制有效性，以主动保护最新和新兴的威胁。

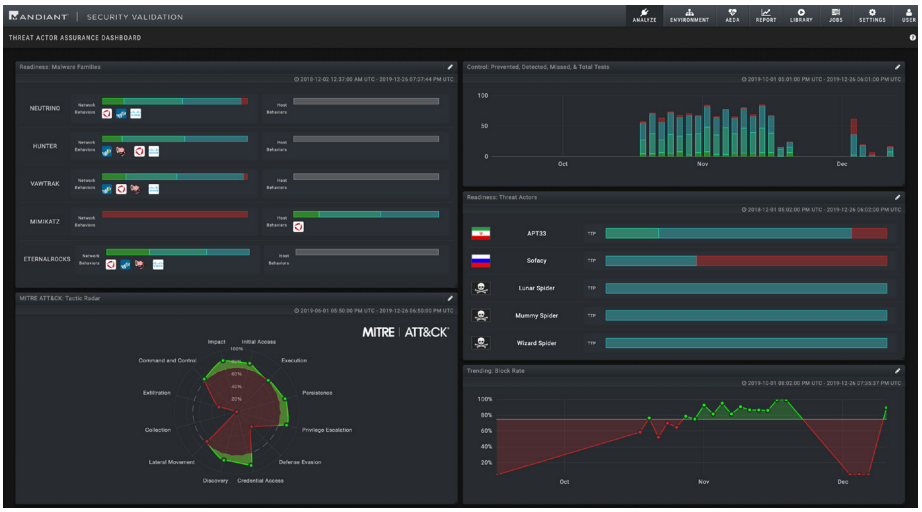

图 3. 威胁参与者保证模块 (TAAM)。

- **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：

- **客户所有和托管模式：**基于云（安全即服务），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，从而一次性评估其防御能力，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。

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 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@FireEye.com

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。

M-EXT-DS-US-EN-000318-02