FIREEYE™

数据表

勒索软件防御评估

优势

- 识别受勒索软件影响的高风险资产
- 识别勒索软件针对的安全漏洞
- 识别文件共享中放松的访问控制
- 认识到勒索软件任务管理中的操作缺陷
- 获得高度可操作性的建议和指导，以减轻勒索软件攻击的影响

为何选择 FireEye Mandiant

自 2004 年起，FireEye 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。我们通过结合对手、设备及受害者情报资源，深入了解威胁制造者及其快速多变的策略、技术及程序 (tools, tactics and procedures, TTP)。

勒索软件防御评估的开发，基于广泛的勒索软件事件响应和修复经验，以及所收集的新兴、不断演变的勒索软件威胁情报。

概要

FireEye Mandiant 勒索软件防御评估可评估组织预防、检测、遏制和补救勒索软件攻击能力的有效性进行评估。Mandiant 专家评估您安全计划的技术和非技术要素，以确定您的团队如何应对勒索软件攻击。

Mandiant 专家可评估勒索软件攻击可能对您的内部网络产生的技术影响，发现哪些数据可能受到危害或丢失，并测试您的安全控制措施在检测和应对勒索软件攻击的能力方面的优势和劣势。

方法论

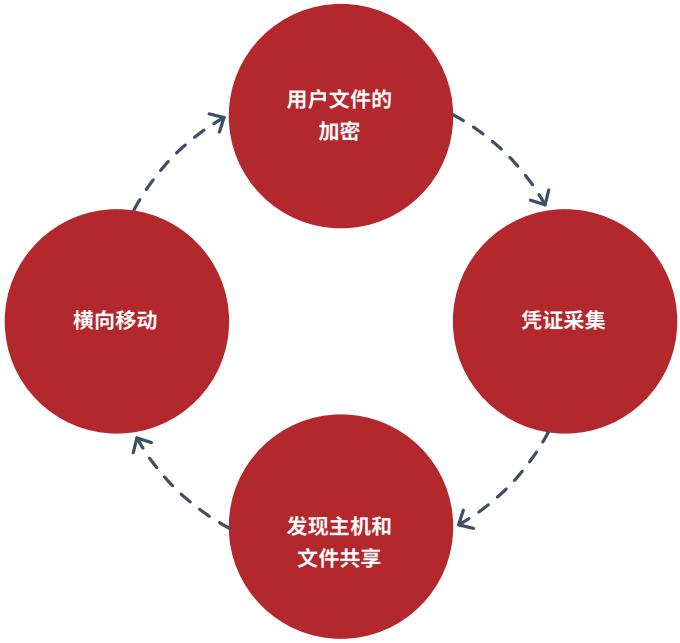
勒索软件防御评估包括文件审查、日志配置分析、深度研讨会和真实勒索软件攻击行为模拟。

勒索软件防御评估侧重于四项核心勒索软件能力：

- **安全架构。**抵御勒索软件攻击并继续业务运营所需的安全技术、控制措施和网络。
- **响应。**组织快速响应和遏制勒索软件攻击的能力。
- **沟通。**用于向关键利益相关者传递企业信息的内部和外部沟通过程。包括与网络安全保险和法律顾问的协调。
- **恢复。**对勒索软件攻击进行补救或恢复的过程和方法。

我们对真实的勒索软件攻击行为进行了模拟：

- 扫描被勒索软件利用的 Windows 漏洞
- 扫描可能被勒索软件访问的可访问文件共享
- 通过尝试利用发现的漏洞或重用所采集的凭证来模拟勒索软件的横向移动
- 测试网络间的分段，以确定勒索软件是否会传播到其他环境，例如：
  - 制造和工厂网络
  - 备份基础设施网络
  - 零售网络
  - 其他安全网络
- 通过使用自定义、非破坏性的勒索软件模拟工具来模拟大规模文件加密，以模拟勒索软件的加密行为
- 执行威胁者用来部署勒索软件的技术



持续时间和交付成果

勒索软件防御评估通常需要一个星期。其可在企业内部或远程执行。

评估结束后，Mandiant 会提供一份报告，其中包括：

- 执行摘要，包括优势和需要改进的领域
- 关于测试过程的技术信息
- 按严重程度分类的详细结果
- 执行简报

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com**

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 FireEye, Inc.

FireEye 是一家情报主导型安全企业。FireEye 为客户提供无缝式、可扩展的讯息安全解决方案，提供一个将创新型安全技术、国家级威胁情报以及闻名于世的 Mandiant® 咨询集成于一体的平台。通过这种方式，FireEye 为殚精竭虑防备、阻止和应对网络攻击的组织，消除了网络安全的复杂性和负担。