McAfee Threat Intelligence Exchange

跨安全解决方案共享威胁情报

McAfee® Threat Intelligence Exchange 就像一个信誉代理，支持适应性威胁检测和响应。它将您组织中的安全解决方案的本地情报与外部、全球威胁数据相结合，并在您的安全生态系统中即时共享这种综合情报，从而支持解决方案交换共享情报和采取行动。

创建协作式威胁情报生态系统

一种信誉代理，McAfee Threat Intelligence Exchange 将导入的全球来源（如 McAfee Global Threat Intelligence (McAfee GTI) 和第三方威胁信息 [如 VirusTotal]）的威胁情报与本地来源（包括终端、网关和高级分析解决方案）的情报相结合。利用 Data Exchange Layer (DXL)，它可以在您的安全生态系统中即时共享这种综合情报，从而让安全解决方案统一运营，在整个组织内增强保护。

集成简单，DXL 支持，大大减少了无数直接应用程序编程接口 (API) 的集成，并可以提供无与伦比的安全、运营效率以及有效性。DXL 采用开放式架构设计，可以使所有安全解决方案动态加入 McAfee Threat Intelligence Exchange 生态系统，包括第三方安全产品。

适应并消除威胁

从网络各个位置检测到的所有共享信息都能促使人们对抵御针对性威胁产生更深刻的认识。由于这些威胁采用精准攻击设计，组织需要运用本地监视系统捕捉趋势及其遭遇的独特攻击。在遭遇攻击时收集的本地环境数据与全球威胁情报结合，有助于更好地确定之前从未见过的文件，从而缩短防护和检测时间。

如果在您的网络上发现无法识别的文件，McAfee Threat Intelligence Exchange 就会通过查询来确定是否存在关于该文件的信誉评分。它还会维护维护组织普及程度以及年限之类的描述性元数据，并且反映在综合情报中。除了请求信誉之外，集成安全解决方案还可以根据本地判断向 McAfee Threat Intelligence Exchange 提供信誉更新。更新的信誉随后会实时传播到您的所有系统中。此应用程序将存储此本地威胁情报以供日后遇到此威胁时使用，这意味着如果再在其他设备或服务器上遇到此威胁，不再会将其视为未知威胁，而会立即检测出此威胁。

管理员可运用 McAfee Threat Intelligence Exchange 轻松地量身打造威胁情报。安全管理员能够组合、覆盖、扩大和优化全面的情报信息，以便为其环境和组织定制保护。此本地确定优先级的微调威胁信息可用于在以后遇到威胁时实现即时响应。

主要优势

- 自适应威胁防护将遭遇高级针对性攻击到遏制攻击的响应过程从数天、数周乃至数月缩短到几毫秒。
- 综合威胁情报是从与收集的本地威胁情报结合的全球情报数据源提炼的情报。
- 相关安全情报可在终端、网关、网络和数据中心安全解决方案之间实时共享。
- 您能够根据终端上下文（文件、流程和环境属性），结合综合威胁情报对前所未见的文件做出决策。
- DXL 简化了调查。通过将 McAfee 和非 McAfee 安全解决方案衔接在一起实时贯彻执行威胁情报，降低实施和运营成本。

强制实施点增强保护

从终端到网络边缘，在全局网络中集成的解决方案可根据可用信誉、元数据或数据点组合应用策略。McAfee Endpoint Security 是一种紧密集成的解决方案，可利用合并的本地情报（文件元数据、如组织普及程度和年限，以及从其他安全组件提交的本地信誉）和当前可用的全球威胁情报来制定准确的决策。例如，没有全球信誉，但有高组织普及程度的自定义应用程序可能不会产生恶意复合信誉，系统很有可能允许它运行。另一方面，对于之前在组织中没有发现过的文件，如果也没有全球或本地信誉，并且打包形式比较可以，那么可能就会产生较低的信任级别，因此可能触发阻止操作，或要求通过 McAfee Endpoint Security 引擎进行深入调查，或要求通过 McAfee Advanced Threat Defense 或 McAfee Cloud Threat Detection 进行沙盒分析。

McAfee Endpoint Security 的 Real Protect 和机器学习能力，以及动态应用程序遏制功能进一步增强了终端检测和保护。Real Protect 利用执行前和执行后分析对最新的威胁情报执行云查询，而动态应用程序遏制功能可阻止终端上的恶意活动，从而在执行额外的分析时保护暴露给新威胁的第一台机器。

协作带来的优势

高级威胁分析

如果需要有关某文件的更多信息，可以将相关信息从 McAfee Threat Intelligence Exchange 自动发送到 McAfee 高级分析解决方案（例如 McAfee Advanced Threat Defense 或 McAfee Cloud Threat Detection），以便立即获取有关新型潜在威胁的更多信息，并确定可疑文件的信誉。所有这些信息都将被自动发送、记录，并通过 DXL 进行集体共享，以便保护您的整个安全生态系统。

安全事件管理

McAfee Enterprise Security Manager 允许您在调查 McAfee Threat Intelligence Exchange 确定的攻陷指标 (IoC) 时执行更深入的分析。历史安全信息访问权限和自动化观察列表创建功能可提高组织的安全防护效率。

高级且具有针对性的攻击一直以来都是现实世界中面临的挑战

高级针对性攻击旨在阻止检测并在组织中潜伏，继而危害阻止并泄露高价值数据。根据近期发布的 Verizon 2015 Data Breach and Investigations Report（Verizon 2015 年数据违规调查报告）数据，70% - 90% 的恶意软件样本都是同一组织唯一的样本，这表明检测唯一的威胁信号是现在最大的挑战。[1]

有关详细信息，请访问 **www.mcafee.com/cn/products/threat-intelligence-exchange.aspx**。

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee Together is power.

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn