McAfee Global Threat Intelligence for Enterprise Security Manager

将 McAfee® Labs 的强大功能引入态势感知中。

McAfee® Global Threat Intelligence for Enterprise Security Manager 将 McAfee Labs 的强大功能引入企业安全监控之中。这是 McAfee Labs 从全球一亿多个威胁传感器收集的 IP 信誉第一次可供安全信息和事件管理 (SIEM) 解决方案使用。McAfee Enterprise Security Manager 这一不断更新的丰富信息源通过快速发现涉嫌可疑或恶意 IP 通信的事件，大大增强了态势感知功能。这样，安全管理员就可以确定哪些主机与恶意用户进行了通信或正在进行通信，从而快速确定威胁活动源自已知恶意用户的情况。

对外部上下文的需求

安全事件实时提供关于安全相关活动的信息。虽然SIEM有能力关联这些事件，但是还有许多问题有待操作人员解决：该活动是否可接受?如何确定哪些事件最为紧急?如何检测深藏不露的复杂攻击?企业典型的日常事件（每季度超过10亿）会让这些问题的数量急剧增加，所以，旧式 SIEM 已知模式的检测显然只是安全监控形势的冰山一角。这背后不为人知的上下文要素中最重要的一个是了解外部系统的信誉。迄今为止，彻底了解安全事件还无法实现。

将 McAfee Labs 的强大功能直接引入 SIEM

McAfee Global Threat Intelligence for Enterprise Security Manager 通过高速且高度智能化的 McAfee SIEM（专为大量安全数据构建）将 McAfee Labs 的强大功能直接引入安全监控流。这一可选订购服务不断传送 1.4 亿多个 IP 地址的来源信誉并进行调整，将外部系统信誉的上下文直接引入安全事件流，从而快速识别出在当前及过去与已知犯罪分子之间的交互活动。利用全球一亿多个传感器和 500 多名研究人员，McAfee Global Threat Intelligence (GTI) IP 信誉从所有主要威胁途径的威胁情报的关联性衍生出来。

主要优势

- 将 McAfee Labs 的强大功能引入 SIEM。
- 准确解读与事件相关的风险。
- 利用 McAfee GTI 的大量威胁源而不影响性能。
- 在 McAfee Enterprise Security Manager 中自动接收和处理新来源信誉。
- 缩短响应时间的同时提高威胁检测准确性。
- 快速识别攻击路径以及过去与已知恶意用户之间的交互活动，往往涉及僵尸网络 (Botnet)、分布式拒绝服务 (DDoS)、用邮件/垃圾邮件发送的用于执行网络探测的恶意软件、恶意软件的存在、DNS 托管及入侵攻击产生的活动。

McAfee Global Threat Intelligence for Enterprise Security Manager 的优势

- **增强对整个网络的保护：**当您的网络上的任何节点与可疑或已知恶意用户通信时，McAfee Global Threat Intelligence for Enterprise Security Manager 可以立即检测到，并且可以快速理解威胁路径。
- **基于风险的优先级：**自动将 IP 信誉纳入 McAfee Enterprise Security Manager 无规则风险评分算法，且自动精确掌握响应需求。
- **全天候 (24/7) 威胁监控：**McAfee Labs 持续搜寻威胁信息以检测新感染情况和恶意系统（在这些系统清理干净时也会进行检测），从而让组织准确了解最新的全球威胁形势。

实时查明恶意活动

现在，凭借 McAfee Global Threat Intelligence for Enterprise Security Manager，组织可以了解任何事件的 IP 信誉，包括异构化防火墙、入侵防御系统、路由器和终端。利用 McAfee Enterprise Security Manager 的动态观察列表功能，事件可以与来源信誉评分直接关联，并且对风险进行调整。随着全球威胁形势的变化，McAfee GTI 会不断更新 McAfee Enterprise Security Manager，确保服务器和系统始终掌握准确的信誉分数。这不仅可以帮助组织了解风险，还可以实时确定紧急问题，缩短事件响应时间窗口并提供准确的风险分析。

找出未知关系

McAfee Enterprise Security Manager 的一个核心优势是可以存储和检索多年的数据，确定这些数据的历史关联性。现在，凭借 McAfee GTI，安全分析师可以实时回溯多年的数据，了解过去与恶意用户的交互。这对检测“底层慢速”攻击、僵尸网络发起的重复性攻击、跨站点脚本 SQL 注入尝试来说至关重要。

缩短响应时间

McAfee GTI 与 McAfee Enterprise Security Manager 警报和报警机制无缝集成，从而确保与已知恶意系统的交互能够引起足够的重视。

由专为大量安全数据构建的 McAfee Database 提供支持

人们对数据变得越来越庞大的现象有过许多讨论，其中也包括将 McAfee Labs 中与安全相关的知识财富引入 SIEM。McAfee Enterprise Security Manager 存储、关联和更新大量 McAfee GTI IP 信誉数据库的功能与众不同，不会造成无法接受的性能影响。McAfee Enterprise Security Manager 具有专用数据库，不仅消除了耗时的 SIEM 数据库管理工作，还经过了精心构建，能够以极高的速度获取和处理大量事件和相关数据。凭借 McAfee Global Threat Intelligence for Enterprise Security Manager，可以让客户对 McAfee GTI 知识的实时交付有信心。

规格

支持的版本

McAfee Enterprise Security Manager 9.4 和 McAfee Event Reporter Appliance 9.4

- McAfee Labs 威胁情报网络：位于全球 120 多个国家/地区的一亿多个节点
- IP 信誉平均值：视具体威胁形势而定

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