运行威胁情报

几乎每个合法警报之后，您的 IT 安全专家接收到的都是使用多项攻击技术侵入您的基础设施和损坏您的重要数据资产或系统的相反效果。今天的攻击性多相攻击包含组成网络攻击链的一系列步骤：侦察、漏洞扫描、漏洞利用和宝贵的企业数据泄露。

安全分析师十分了解这些技术，并借助威胁情报来深入了解攻击方法和动机。他们可以检测和中断高级威胁下载，采用恰当的补救措施，为下一次发出安全警报的情况更好地做好补救准备。但是，他们经常都是缺乏对特定系统的监控或被大量数据和少量情报干扰。美国系统网络安全协会研究表明，《Who's Using Cyberthreat Intelligence and How?》（谁正在使用网络威胁情报以及如何使用？），“…仅 11.9% 的受访者可以从几乎各种来源收集威胁信息，而且仅 8.8% 受访者可以利用攻陷指标结合事件全面地认识威胁情报。”[1]

在近期的报告中，Forrester 指出，77% 的北美和欧洲企业安全性决策者报告称，提高威胁智能感知系统功能具有最高优先级。[2] 网络威胁情报承诺针对网络犯罪分子攻击他们的地区、行业甚至是特定公司的情况提前向安全从业人员发出警告，这样他们就有时间采取措施进行抵御，但是 IT 安全专家仍然要面对一些大的挑战：

- 如何从外部和内部源收集威胁情报。
- 如何关联数据并区分风险优先次序。
- 如何在多供应商安全控制企业范围分布情报。
- 如何加大对 IT 威胁形势的监控力度，以便迅速地采取恰当的措施。

现代企业需要一个开放式集成架构，可以简化威胁情报的使用流程，并让他们享受收集签证的基本威胁数据并用来丰富 SIEM 分析带来的优势。换句话说，用户需要通过自动化流程将威胁情报投入使用，这样有助于分析、融会贯通和管理威胁情报。

新威胁需要威胁情报采用新的抵御方法

随着攻击的复杂性、精准度和数量的增加，之前采用的威胁情报抵御方法已不满足不了当前形势的要求。调查针对性攻击不是一件简单的任务。攻击者的动态行为、本地和全局威胁情报源多样性和可用性的不断增加以及威胁情报数据格式的多样性会使将威胁情报汇总并融会贯通到安全运营中心 (SOC) 相较于之前面临更大的挑战。

混合供应商环境是大多数企业面临的一种常见环境，其增加了在整个企业中共享事件数据和加强事件监控力度的难度。Gartner 在其报告《Technology Overview for Threat Intelligence Platforms》（威胁情报平台的技术概述）指出，“企业无法共享 TI 为网络威胁犯罪分子提供了便利条件。TI 共享会使威胁抵御能力倍增，已经成为与日益增加的威胁犯罪分子数量以及他们使用的攻击保持同步的关键因素。”[3]

“对于我们的安全基础设施，我们需要的不只是技术供应商。很明显，我们要跟可以协助我们管理多样化用户要求和不断变化的威胁状态的合作伙伴建立合作关系。迈克菲构建了这种合作伙伴关系，我们从 McAfee 解决方案获得的持续安全情报在帮助保持业务运营的前沿性方面尤为重要。”

—Anurana Saluja CISO，Sutherland Global Services 信息安全副总裁

但是，只共享威胁情报不一定会导致采用持续的纠正措施和抵御方法。安全分析师会因过多的信息很快就被弄得一头雾水。大多数安全团队采用的都是全手工流程（参见图 1）对数以百万计的安全事件和可疑文件进行分析，旨在将大量数据汇总在一起，并尝试重建针对性攻击。这样最终会破坏响应流程的全面性并减缓响应速度。由于对威胁的了解不全面，安全团队正在努力及时地收集各类攻击。根据最新研究，Intel Security（现在称为 McAfee）：《When Minutes Count》（分秒必争，抵御威胁），2014，25% 以下的受访者曾说过，他们可以在数秒内检测到攻击。[4]

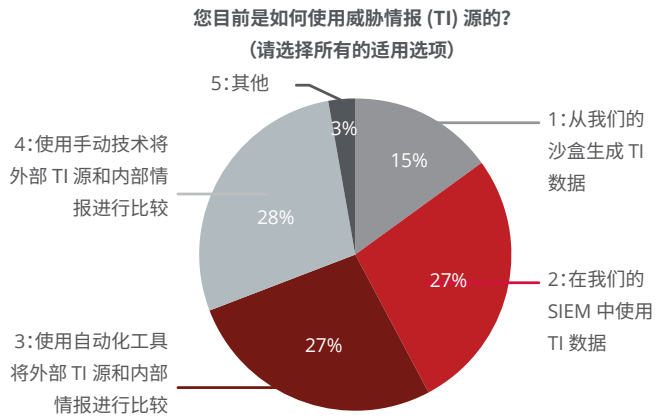

图 1. 根据 BlackHat 2015 期间展开的 Intel Security（现在称为 McAfee）调查，大部分用户仍然采用手动技术来对比外部威胁情报源和内部威胁情报。

运行威胁情报

情报主导式威胁检测和补救不只需要每周一次手动将开放式网络上发布的破坏性 IP 地址导入到 SIEM 观察列表中。相反，其需要收集实时威胁情报并关联攻击的各个方面，包括方法和全球活动，这样企业甚至可以预先制止隐匿程度最高调整速度最快的威胁。企业 SOC 需要采取某种方法来“运行威胁情报”，以便全面了解影响他们环境的各类攻击。他们需要采取某种方法来筛选大量的数据，以便对威胁情报进行分析、关联和优先排序，并确定与他们的行业、地理位置和公司的关系。而且，他们需要能够了解目前可能发生的独特攻击，以及了解基于历史安全事件数据的趋势。如 Forrester 指出，运行威胁情报很重要，因为 75% 的攻击会在 24 小时内从一个受害者蔓延到下一个受害者。企业需要缩短“共享速度和攻击速度”之间的时间间隙。[5]

利用 McAfee 的集成架构

McAfee 提供统一的协作平台，该平台具备运行威胁情报的所有组件，包括全局威胁情报源、本地情报创建、实时共享 IT 基础设施、安全信息和事件管理之间的威胁信息以及传送自动的自适应威胁防护。

威胁情报要求	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
从外部源收集威胁情报	STIX、McAfee® Global Threat Intelligence (McAfee GTI) 导入和 VirusTotal	McAfee GTI 导入	通过网络威胁经理的 McAfee Enterprise Security Manager McAfee GTI、TAXII/STIX 导入和 HTTP 威胁源	McAfee GTI 汇总来自多个网络 Cyber Threat Alliance 合作伙伴和公共源的威胁情报。McAfee GTI 从客户所部署 McAfee 产品上的数百万台传感器（如终端、Web、邮件、网络入侵防御系统 (IPS) 和防火墙设备）中提取威胁情报
收集内部威胁情报	从 McAfee VirusScan®、McAfee Application Control、McAfee Web Gateway、McAfee Advanced Threat Defense 和 McAfee Enterprise Security Manager 以及从在 Data Exchange Layer 上发送信息的第三方供应商产品上收集样本	从 McAfee Threat Intelligence Exchange 或通过网络利用爆炸样本文件	通过 STIX/TAXII 和 Data Exchange Layer	
生成本地威胁情报	记录可疑文件事件，并创建记录威胁的首次接触和轨迹的本地数据库	剖析和证实恶意软件存在犯罪，生成本地威胁情报，并分布到 Data Exchange Layer 或分布为 STIX 格式 API	基于关联事件创建威胁情报观察列表、报告和观点	
在安全控制范围内分布威胁情报	利用 Data Exchange Layer	利用 Data Exchange Layer 和产品 API	利用 Data Exchange Layer、产品 API 和脚本集成	McAfee GTI 与众多 McAfee 产品集成，如 McAfee Web Gateway、McAfee Enterprise Security Manager 和迈克菲终端解决方案
监控收集到的威胁情报	利用 McAfee Threat Intelligence Exchange 信息显示板	利用报告	利用内容包中提供的信息显示板、观点和报告或用户生成的数据	利用 McAfee Threat Center 以及每季度的迈克菲威胁报告

表 1. McAfee 的集成威胁情报平台

获取、分析和传播

McAfee Global Threat Intelligence

开始构建您的集成威胁情报平台的最好选择就是 McAfee Global Threat Intelligence (McAfee GTI)，基于云的全方位实时信誉服务完全集成到了 McAfee 产品中，使这些产品能够更好地迅速地抵御所有媒介（文件、Web、消息和网络）中的网络威胁的侵扰。McAfee GTI 基于从多个源收集到的威胁数据对数十亿文件、URL、域和 IP 地址进行信誉评分，这些源包括：McAfee Labs 监控和分析的全球范围内的数百万个传感器、研究合作伙伴提供的威胁源、利用 Cyber Threat Alliance 以及来自 Web、电子邮件和网络威胁数据的跨媒介情报。凭借高品质的相关威胁源，McAfee GTI 可提供准确的风险应对建议，可促进制定知情策略，让控件根据需要阻止、清理或允许威胁侵入。

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (SIEM) 最大限度地发挥安全情报获取和分析的作用，提供每种威胁情报类型的整合、分析和操作核心。这种全方位监控允许全面监控和态势感知检测和响应针对性攻击的速度。其高级数据管理系统旨在实时存储和添加大量的环境数据。

McAfee Enterprise Security Manager 从您的所有系统、数据库、网络和应用程序收集活动和事件数据。它还会导入全球威胁源，并以标准格式（例如 Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) 和 Cybox）利用和传输威胁情报，这些资源通常由社区或行业组织（如 Financial Services Information Sharing and Analysis Center (FS-ISAC)发布。

通过高级分析，它会将收集到的信息转换成便于理解和使用的安全情报。更重要的是，它可以通过实时视图和访问历史安全信息来更深入地监控新涌现的威胁。这就可以让您及时调查以往的事件，了解攻击的流行状况和模式，同时也可以创建自动关注列表来检测以后发生的事件或重复发生的事件。通过加强系统对已知恶意事件的敏感度，您可以提升在攻击链的不同阶段检测可疑活动和活动模式的能力，然后确定响应优先次序。

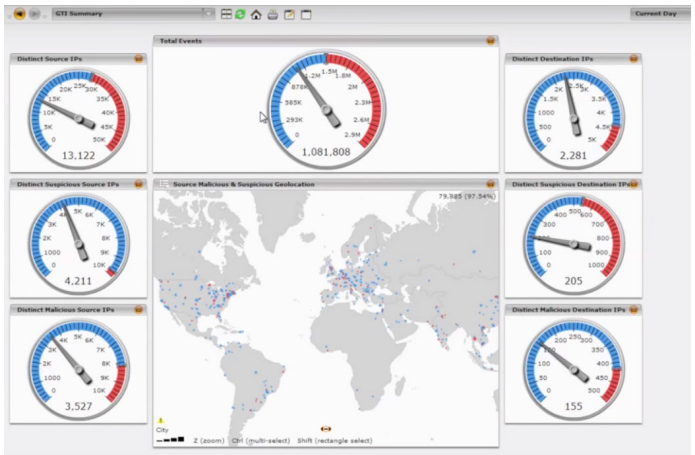

图 2. McAfee GTI 视图。

什么是 Cyber Threat Alliance?

Cyber Threat Alliance 是一组从企业中选出的网络安全从业人员，他们相互合作以共享威胁信息，并帮助提高抵御跨成员企业及其客户的对手攻击的能力。McAfee 是创始成员之一,这些成员有专门的资源来确定共享威胁数据，以最有效的方式促进成员之间相互协作，并制定统一的流程来抵御复杂的网络犯罪活动。

McAfee GTI for McAfee Enterprise Security Manager 为企业安全监控提供了强有力的 McAfee Labs 研究功能。通过启用事件快速发现功能（包括与可疑或恶意 IP 的通信），这种不断更新的丰富的 McAfee GTI 源可增强态势感知功能，并且可让安全管理员确定与哪些企业主机通信或哪些主机最近与已知犯罪分子通信。

McAfee Threat Intelligence Exchange

在开发集成的威胁情报生态系统时，您可以添加的第三个组件是 McAfee Threat Intelligence Exchange，它会在整个安全基础设施中汇集和共享文件信誉情报。McAfee Threat Intelligence Exchange 可接收来自 McAfee GTI、STIX 文件导入和通过 McAfee Enterprise Security Manager 获得的威胁源的威胁信息，以及来自终端、应用程序控制、移动设备、网关和数据中心的信息，还有 McAfee 解决方案及其他供应商提供的解决方案的沙盒技术。

从您的基础设施中的所有点收集数据可以提供可能只会在您的环境中出现的威胁的相关信息，多数针对性攻击就是这样。这样，文件信誉信息可即时通过 Data Exchange Layer (DXL) 与连接到McAfee Threat Intelligence Exchange 的所有产品和解决方案的整个生态系统共享。例如，如果 McAfee Threat Intelligence Exchange 推送与恶意可执行文件相关的信息，McAfee Data Loss Prevention 会通过 DXL 接收此类信息，然后开始监控这些意在进行敏感文件访问的可执行文件。

通过 DXL 共享的威胁数据包括文件信誉、数据分类、应用程序完整性以及用户上下文数据，这些数据在集成到 DXL 结构中的产品之间和之中共享。所有产品或解决方案都可集成到 DXL 上，然后对其进行配置，以确定要发布到系统中，要侦听和要订阅的信息。

McAfee Threat Intelligence Exchange 与高级沙盒解决方案 McAfee Advanced Threat Defense 紧密结合，可为 McAfee Threat Intelligence Exchange 提供恶意软件分析数据。如果发现文件是恶意的，McAfee Threat Intelligence 会向所有通过 DXL 连接的系统推送文件信誉更新。这反过来也可以发挥作用。当启用了 McAfee Threat Intelligence Exchange 的终端遇到信誉未知的文件时，可以将文件提交给 McAfee Advanced Threat Defense，以确定该对象是否具有恶意，从而消除带外负载传输的盲点。上述两种产品协同工作，提供自动的自适应防护措施抵御新涌现出的威胁。有关已发现攻击的信息会在您的环境中传递，从而帮助阻止网络攻击链，以免造成更大的损失。

McAfee Threat Intelligence Exchange 通过实时利用跨终端、网关、网络和数据中心安全解决方案的执行情报，从而实现自适应威胁检测和响应。通过结合导入的全球威胁信息和本地收集的情报并即时共享，让您的安全解决方案作为一个整体运行，从而交换共享情报并根据这些情报采取行动。

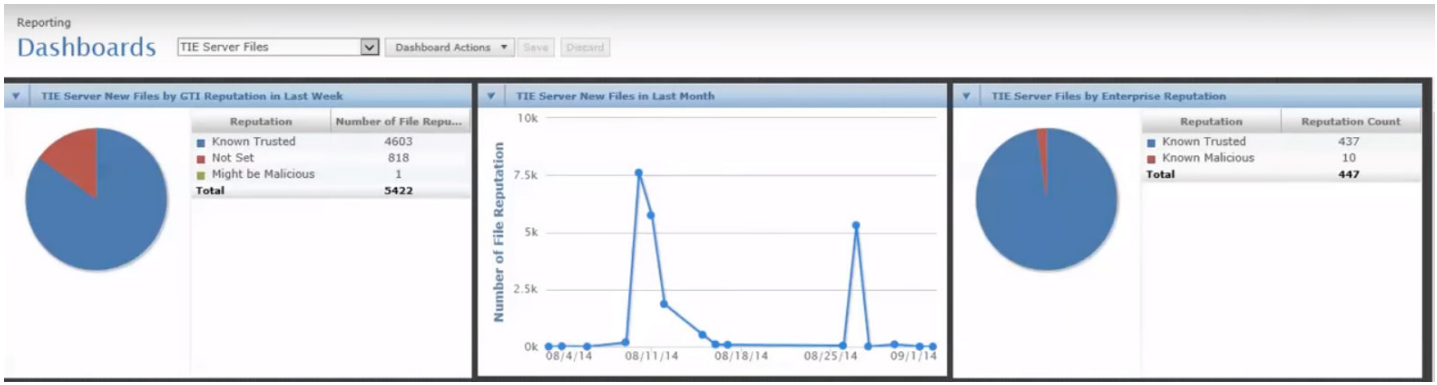

图 3. McAfee Threat Intelligence Exchange 信息显示板

中断网络攻击链

无论未知恶意软件文件发生的首个接触点在何处，一旦证实文件存在恶意，将立即更新整个连接环境。当 McAfee Advanced Threat Defense 证实文件存在恶意时，McAfee Threat Intelligence Exchange 会通过信誉更新发布确认信息，即通过 DXL 传输到所在企业中的所有安全控制机制。启用 McAfee Threat Intelligence Exchange 的网关可以防止文件进入您的基础设施。通过在所有安全控制机制中协调共享威胁情报，使中断攻击链和避免进一步损害变得更加轻松，无需手动干预。

消化并应用：根据准确性进行检测并制定更加明智的决策

在使用威胁数据之后，McAfee Enterprise Security Manager 作为中心监控点，将 McAfee GTI、McAfee Threat Intelligence Exchange 源以及 STIX/TAXII 格式攻陷指标 (IoCs) 与事件数据（实时检测到的事件数据或之前网络上的节点与已知犯罪分子或可疑域进行通信的相关数据）进行关联。威胁管理信息显示板会为分析师全面显示收集到的威胁指标、资料源、指标命中率以及与攻陷指标 (IoCs) 相关的最重要的用户可读详细信息。

结合其他协作性威胁情报工具一起使用 McAfee SIEM 系统可降低与配置关联规则（通常是十分繁琐的手动操作流程）相关的运营支出。例如，安全分析师可以在用户可读格式中直接查看新接收到的威胁信息，从而更好地了解新检测到的威胁。更重要的是，可通过实时或历史关联规则自动使用接收到的威胁情报，从而缩短检测正在进行的或新的侵扰活动所需的时间。用户也可以按照在整个 IT 环境报告威胁的进度，以及通过警报视图中的上下文信息，制定更加明智的决策。上述所有收集到的情报都可以改进和加快检测和调查针对性攻击。

以下 McAfee 产品支持 STIX 格式威胁情报：

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

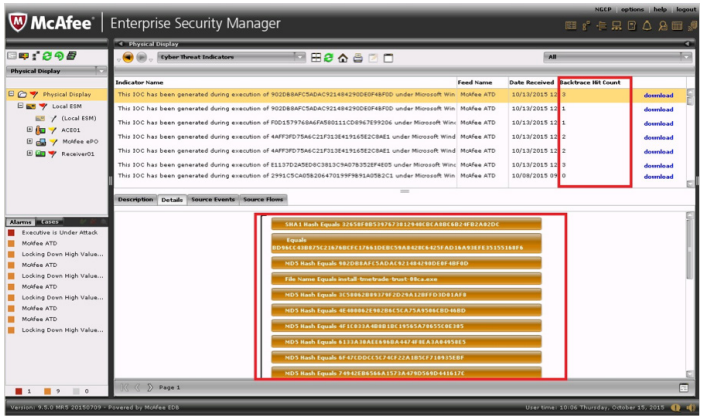

图 4. McAfee Enterprise Security Manager 网络威胁指标回溯命中和 IoC 威胁详细信息。

由于威胁迅速蔓延到 IT 基础设施且会随着时间而发生变化，McAfee Enterprise Security Manager 可以定期刷新所有获取到的威胁情报，从而消除旧的、关联性较小的数据。例如，自动清空已删除的命令、控制服务器或恶意信誉评分较低的安全网站，以便消除可能会分散安全工作人员的注意力，使其不能追寻真凶的误报。

总结

McAfee 的集成威胁情报用于实施威胁情报的获取、吸收和管理，可让您提高威胁检测的准确性，消除手动操作的辛苦，并阻止敌手损害您的企业。通过改进监控里并加强对整个安全生态系统的观察，能够更好地为识别和预先制止当前的针对性攻击并避免接下来出现这些攻击做好准备。

了解更多信息

有关构建 McAfee 的集成威胁情报平台的更多信息，请访问：

- McAfee Global Threat Intelligence
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Enterprise Security Manager
- How to Use a TAXII Feed with McAfee Enterprise Security Manager (如何同时使用 TAXII 源和 McAfee Enterprise Security Manager)

1. https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767
2. https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011
3. https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms
4. http://www.mcafee.com/cn/resources/reports/rp-when-minutes-count.pdf
5. https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf

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