McAfee Investigator

让分析人员变成调查专家

McAfee® Investigator 可以增强分析师的信心，帮助他们更快速地终结更多需要确定根本原因的案例。分类警报触发由专家带领的如下探索：收集支持数据、解释证据以及展示快速彻底地验证威胁并做出响应所需的见解。

安全运营挑战

庞大的事件数量和数据储存期问题导致难以准确评估警报的重要性和范围。分析师通常会忽略警报，因为他们缺少确定是否将警报当做正式事故的上下文信息和知识。

因此，任何特定事故的调查都可能需要大量时间和专业知识，需要分析大量威胁载体才能找到问题的核心。这些趋势意味着对优秀安全运营分析师的需求正在急剧增长，而这方面的人才十分短缺。

新调查分析方式

要处理这一问题，安全运营团队需要简化和加快警报分类与调查，从而使他们现有的员工和初级分析师能够完成更多工作。

McAfee Investigator 在每个安全运营团队可触及的范围内提供了包含分类、全面数据收集和高级分析在内的指导性调查。作为 SaaS 服务，专家系统与终端捕获工具与现有数据源和安全管理系统集成，以快速实现价值并最大限度减少工作量。

这些交互式分析方法可以提供持续更新的指南，帮助事故响应人员全面调查恶意软件、网络威胁和攻陷指标 (IoC)，缩短调查时间并提高准确性。

以机器速度发现见解

通过允许安全运营自动划分需要立即注意的特定情况的优先级，McAfee Investigator 可以即时改善分类。对于需要分析师研究的这些报警以及其他警报，McAfee Investigator 会收集、整理和可视化为可以攻击收集的警报、活动、证据以及情报。

主要优势

- **缩短停延时间：**彻底研究案例数据可以改善根本原因检测，而不是修正症状。
- **从警报转变成案例：**减少在人工和低优先级调查方面花费的时间。
- **关注未知问题：**关注需要人类解释和制定决策的独特项目和见解。
- **改善分类：**以更快的速度和更高的质量处理更多案例。
- **减轻分析师疲劳：**高效利用有限的时间、能量和认知能力。
- **培养分析师技能：**指南和相关见解可以培养分析师对工作流提出正确的问题和假设的能力。
- **提高当前系统的价值：**增强现有数据源和分析，提高专注度和准确性。

在后台收集相关数据，并且仅包括将触发决策的特定威胁调查的重要见解。安全信息和事件管理 (SIEM) 解决方案的数据可以通过终端数据进行扩展，无需每个节点的终端检测和响应 (EDR) 代理。该模型利用 IoC、策略、技术、程序和关系方面具备上下文的可见性来替换孤岛。

数据分析和机器学习引擎将证据数据与已知基准和威胁情报源进行对比，从而处理遗留项并提出关键可疑见解。

通过自动收集正确的数据并划分优先级，McAfee Investigator 可以减少工作，提高速度，从而让分析师准确判断事故的风险和紧迫程度。分析师可以更快速的制定准确的分类策略，并集中精力处理最重要的威胁。

对于组织级别，优势更大。通过将警报审核的分类升级到上下文案例，可以提高每个分析师的效率，并且第 1 层分析师可以处理更多案例，同时将分析师时间用再高价值活动上。

利用专家知识指导调查

当选定要进行详细调查的事故后，分析师在确定范围和评估时可以利用交互式指南集中精力分析重要的威胁。调查指南并非基于脚本或一成不变的资源。该系统模拟人类思维过程，可以并行研究许多假设情况，实现最快的速度和准确性。

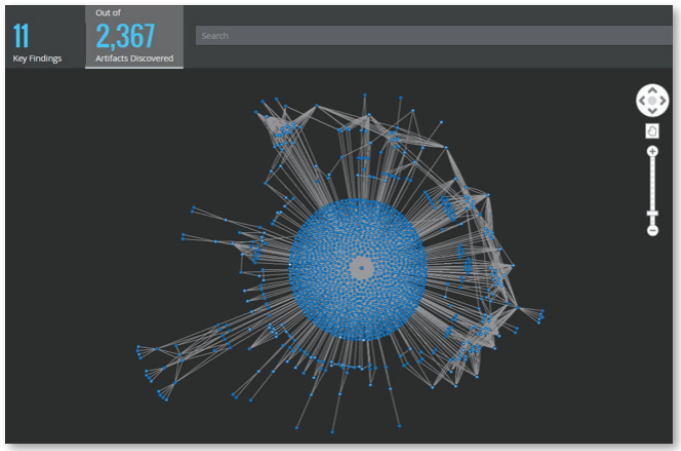

图 1. McAfee Investigator 收集成千上万的分散式证据。

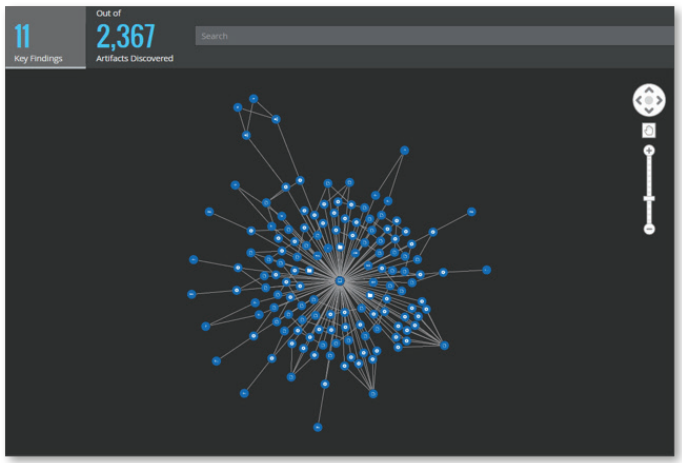

图 2. McAfee Investigator 随后运用专家分析和指南来提供相关的发现。

主要功能

- 按需准确收集数据
- 临时终端收集代理
- 根据专家指南和人工智能解释收集的数据
- 交互式可视化
- 多方位假设研究类似数据
- 机构情报的基准
- 案例管理在整个调查过程中为员工提供指导并允许共享信息

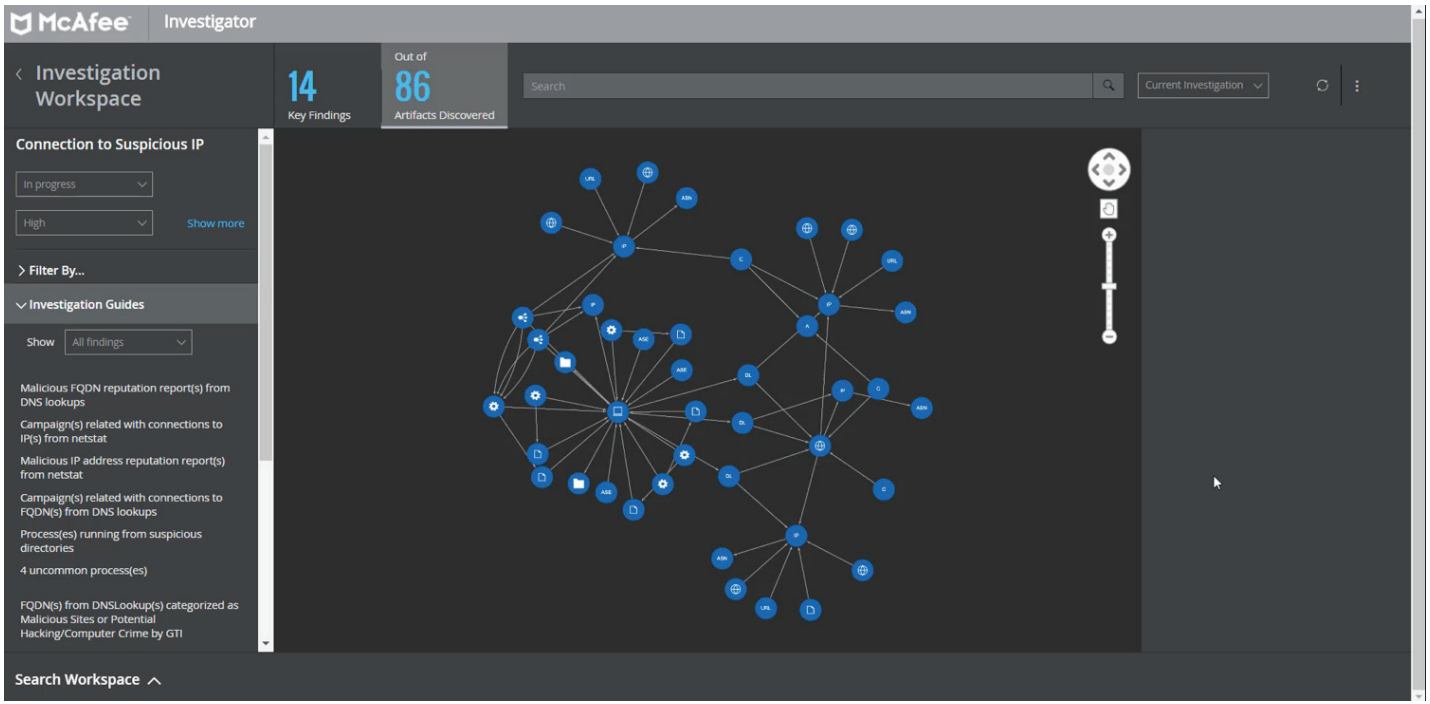

图 3. 工作空间凸显并简化关键发现的研究。

人类可读指南利用 Foundstone® 研究人员的专业知识和人工智能创建而成。这是体现了 McAfee Investigator 人机团队性质的一个方面。

工作空间可以组织案例见解和发现，从而帮助分析师提出正确的问题。凭借分析师已经确定根本原因的高可信度，这种集中、多方位的研究可以高效而准确地结束案例。

扩充专业技能和能力

McAfee Investigator 的交互式工作区可以提示工作流，并让调查人员在单一认知环境中浏览数据。该模型提高了效率并减少了从众多警报类型收集信息的负担，同时还消除了查看多个屏幕的必要性。

该工作区可以引导初级和中级分析人员实现高级分析人员的思维流程，无需单独的培训即可培养技能。

构建现有工具和数据

McAfee Investigator 与 SIEM 和 McAfee® ePolicy Orchestrator® 软件相结合，将高级分析功能添加到现有数据源、基准、关联和警报。临时代理可以收集对准确解释细微证据而言至关重要的新终端数据。通过将 McAfee Investigator 与 McAfee Active Response 相集成，可以让分析师实时确定威胁在其终端中的影响范围。活动源可与第三方工具共享数据，以便将这些数据插入到当前工作流程中，从而简化流程并改善协作。专业服务可以加速参与和成功激活。

了解更多信息

利用 McAfee Investigator，发现可疑情况后，您无需花数小时来收集数据和更多时间来解释数据。McAfee Investigator 的后台高级分析引擎可以在基于上下文的界面中检查和分类威胁警报，从而调适安全操作。McAfee Investigator 在 SOC 调查中自动利用专业知识，让您的分析师可以更加聪明、快速而准确的工作。

这就是人机协作。

请访问 **www.mcafee.com/cn/products/investigator.aspx** 了解详细信息。

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

2018 年 5 月