McAfee Investigator

Превращаем аналитиков в специалистов по расследованию угроз

McAfee® Investigator помогает аналитикам повысить скорость разрешения проблем и быть более уверенными в том, что им удалось определить действительную причину той или иной проблемы. Приоритизированные предупреждения позволяют специалистам детально изучить проблему благодаря сбору сопутствующих данных, анализу информации и предоставлению подробностей, необходимых для полного и быстрого выявления и устранения угроз.

Проблемы обеспечения безопасности

Огромное количество событий и проблемы, связанные со «сроком годности» данных, сильно затрудняют задачу точной оценки степени важности и масштабности того или иного предупреждения. Аналитики часто игнорируют предупреждения, потому что для принятия решения о наличии формального инцидента им не хватает контекста или знаний.

Чтобы докопаться до сути проблемы при расследовании любых отобранных инцидентов, может потребоваться много времени, глубокие специальные знания и опыт противодействия всем факторам угроз. Получается, что потребность в опытных аналитиках по обеспечению безопасности растет, а количество имеющихся специалистов — нет.

Новые средства расследования

Для решения этой проблемы специалистам по обеспечению безопасности необходимо оптимизировать и ускорить приоритизацию предупреждений и расследование, чтобы имеющиеся сотрудники и младшие аналитики могли выполнять больший объем работ.

McAfee Investigator делает направляемые расследования, включающие в себя приоритизацию угроз, комплексный сбор данных и расширенную аналитику, доступными для всех отделов, занимающихся операциями по обеспечению безопасности. Интеграция предлагаемых в виде «ПО как услуга» (SaaS) экспертных систем и средств захвата конечных точек с уже имеющимися источниками данных и системами управления

Ключевые преимущества

- **Сокращение времени пребывания угроз в системе.** Тщательное изучение собранных данных повышает вероятность того, что будет выявлена основная причина проблемы, а не просто устранены ее симптомы.
- **Приоритизация не предупреждений, а ситуаций.** Это позволяет сократить объем расследований, имеющих низкий приоритет и выполняемых вручную.
- **Возможность сосредоточиться на неизвестном.** Аналитики могут сосредоточиться на уникальных артефактах и результатах анализа, требующих внимания человека.
- **Оптимизация процесса приоритизации.** Аналитики могут повысить скорость и качество обработки ситуаций.
- **Снижение риска «выгорания» аналитиков.** Время, энергия и когнитивный потенциал — ограниченные ресурсы, требующие оптимального применения.

безопасностью позволяет сократить срок окупаемости инвестиций и минимизировать трудозатраты.

Эти интерактивные средства анализа дают специалистам по реагированию на инциденты возможность быстрее и точнее расследовать вредоносные программы, сетевые угрозы и признаки взлома, используя постоянно пополняемый набор рекомендаций.

Обнаружение причин со скоростью работы компьютера

McAfee Investigator обеспечивает мгновенное улучшение результатов приоритизации, так как дает центру SOC возможность автоматизировать приоритизацию определенных ситуаций, требующих немедленного внимания. По таким оповещениям, а также по другим предупреждениям, которые хочет изучить аналитик, McAfee Investigator собирает, организует, резюмирует и визуализирует всю имеющуюся информацию (предупреждения, действия, доказательства, данные о предполагаемой атаке).

Сбор необходимых данных осуществляется в фоновом режиме. При этом собираются только те данные, которые необходимы для принятия решения по конкретной расследуемой угрозе. Данные из систем управления информацией о безопасности и событиями безопасности (SIEM) могут дополняться данными, получаемыми с конечных точек, причем для этого не нужно устанавливать на каждом узле агент EDR (endpoint detection and response — технология обнаружения угроз и реагирования на инциденты на конечных точках). Такая модель позволяет заменить

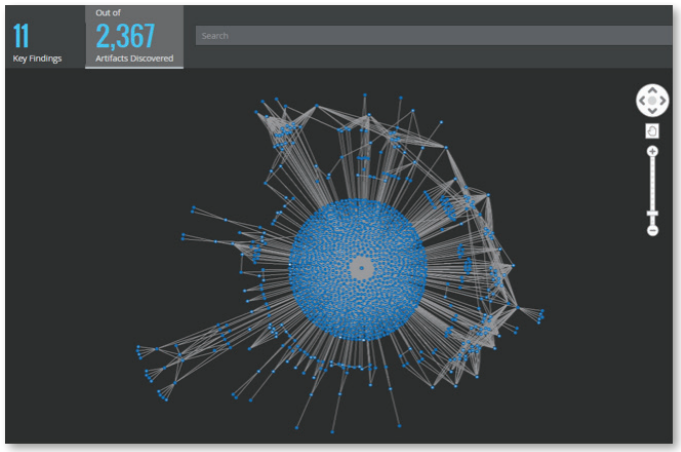

Рис. 1. McAfee Investigator собирает тысячи разных улик.

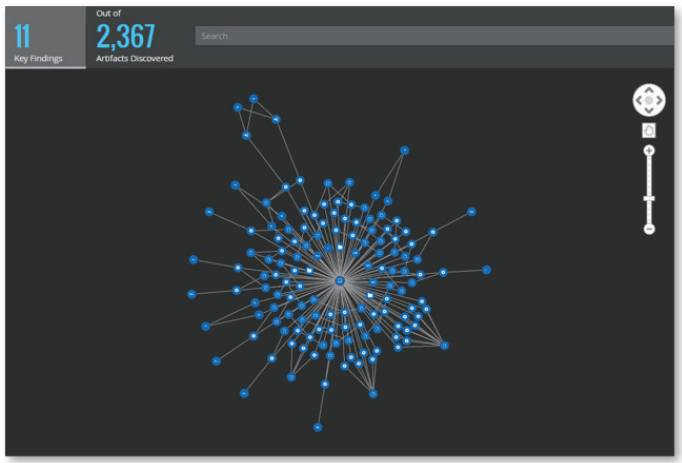

Рис. 2. Затем, используя специализированные средства анализа и опираясь на рекомендации экспертов, McAfee Investigator представляет только те результаты, которые важны.

Ключевые преимущества (продолжение)

- **Развитие аналитических навыков.** В распоряжение аналитиков предоставляются специальные руководства и информация о том, какие вопросы следует задавать и какие гипотезы выдвигать в ходе работы.
- **Повышение отдачи от уже имеющихся систем.** Дополнение уже имеющихся источников данных и средств анализа позволяет повысить эффективность и точность работы.

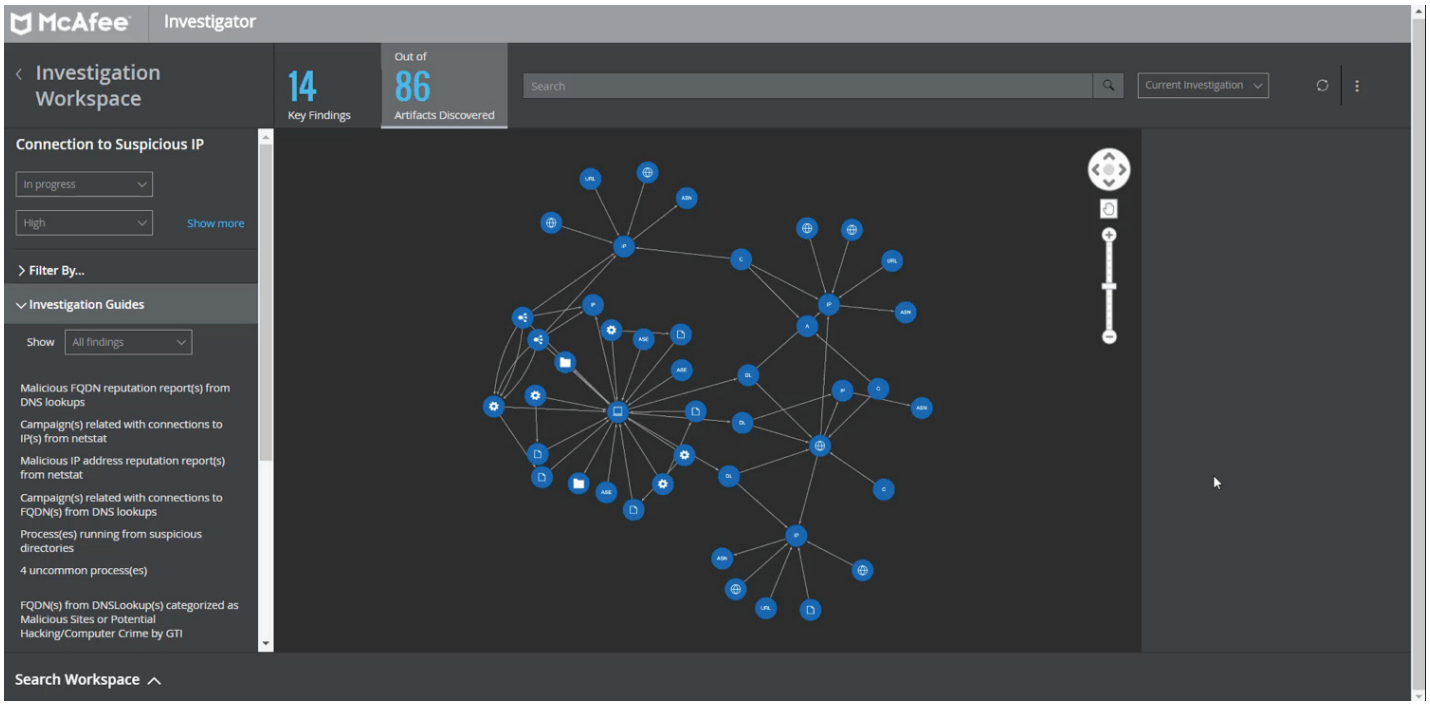

Рис. 3. Рабочая среда облегчает задачу просмотра и понимания основных результатов анализа.

Ключевые функции

- Точный сбор данных по требованию
- Временный агент для сбора данных на конечных точках
- Интерпретация собранных данных с опорой на рекомендации экспертов искусственного интеллекта
- Интерактивные визуализации
- Многовекторные гипотезы для изучения вероятных данных
- Базовые уровни для сбора информации внутри организации
- Механизм управления ситуациями, который задает направление действий сотрудников и позволяет обеспечить обмен информацией в процессе расследований

изолированные системы безопасности системой сбора контекстной информации о признаках взлома, тактиках, методах, процедурах и отношениях.

Модуль анализа данных и машинного обучения сравнивает собранные данные с известными базовыми показателями и полученной из разных источников информацией об угрозах. Он обрабатывает артефакты и выделяет основные подозрительные моменты.

Благодаря автоматическому сбору и приоритизации правильных данных McAfee Investigator дает аналитикам возможность снижать трудозатраты и быстрее определять степень серьезности и неотложности инцидентов. Аналитики тратят меньше времени на принятие точных решений по приоритизации и могут сосредоточиться на самых важных инцидентах.

В масштабах организации преимущества растут в геометрической прогрессии. Переход от приоритизации просматриваемых предупреждений к приоритизации контекстных ситуаций («кейсов») позволяет повысить производительность труда каждого аналитика, увеличить количество ситуаций, разрешаемых аналитиками 1-го уровня, и использовать время аналитиков с максимальной отдачей.

Координация расследований на базе экспертных знаний

Выбрав для подробного изучения тот или иной инцидент, аналитики могут обратиться к специальным интерактивным руководствам, помогающим правильно расставлять приоритеты при формулировании задач и проведении оценок. Руководства по расследованию инцидентов не носят характер «сценария» или статичного предписания. Система имитирует мыслительный процесс человека, ведя параллельную проверку большого количества разных гипотез, что позволяет обеспечить максимальную скорость и точность работы.

Руководства, представленные в удобной для восприятия форме, создавались совместными усилиями сотрудников Foundstone® и систем искусственного интеллекта. Это один из примеров того, как в McAfee Investigator реализован принцип совместной работы человека и машины.

Рабочая среда структурирует информацию о ситуации и помогает аналитикам задавать правильные вопросы. Целенаправленное многовекторное изучение данных помогает закрывать инциденты эффективно, точно и с высокой степенью уверенности в том, что аналитикам удалось определить действительную причину проблемы.

Масштабируемые экспертные знания и возможности

Интерактивная рабочая среда McAfee Investigator позволяет управлять рабочими процессами и просматривать данные в едином когнитивном пространстве. Такая модель позволяет повысить эффективность и снижает информационную нагрузку, возникающую при использовании большого количества разных типов предупреждений. Кроме этого, она избавляет вас от необходимости вести мониторинг на различных экранах.

Рабочая среда служит новичкам и аналитикам среднего уровня своего рода наставником, учащим их думать как опытные аналитики и дающим им возможность развивать свои навыки без прохождения специального обучения.

Использование уже имеющихся средств и данных

Взаимодействие с SIEM и программным обеспечением McAfee® ePolicy Orchestrator® дает McAfee Investigator возможность дополнять имеющиеся источники информации, базовые уровни, корреляции и предупреждения новыми, расширенными аналитическими данными. Для сбора «свежих» данных на конечных точках используется временный агент. Такие данные особенно важны для точной интерпретации неявных улик. Интеграция McAfee Investigator с McAfee Active Response позволяет аналитикам оценить опасность угрозы на конечных точках в реальном времени. Веб-канал активности передает данные инструментам третьих сторон, чтобы они могли подключиться к текущим рабочим процессам. Тем самым обеспечивается оптимизация процессов и совершенствуется совместная работа. Для ускорения адаптации сотрудников и успешной активации продукта можно воспользоваться услугами наших специалистов из подразделения профессиональных услуг.

Дополнительная информация

McAfee Investigator избавляет аналитиков от необходимости часами собирать и интерпретировать данные при наличии подозрения. Используемый в McAfee Investigator передовой аналитический модуль осуществляет изучение и приоритизацию предупреждений об угрозах внутри контекстного интерфейса, позволяющего масштабировать операции по обеспечению безопасности. McAfee Investigator автоматизирует процесс использования экспертных знаний при проведении расследований в центрах SOC, что дает аналитикам возможность повысить эффективность, скорость и точность своей работы.

Это и есть совместная работа человека и машины.

Дополнительную информацию см. по адресу **www.mcafee.com/ru/products/investigator.aspx**.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/ru