McAfee Active Response

Комплексное средство обнаружения угроз и реагирования на инциденты для защиты конечных точек

Ключевые преимущества

- **Автоматизация:** захват и отслеживание изменений контекста и состояния системы, потенциально являющихся ПА, а также обнаружение бездействующих компонентов атаки и рассылка информации об угрозах аналитикам, в отдел эксплуатации и специалистам по проведению компьютерно-технических экспертиз.
- **Адаптируемость:** у пользователя есть возможность адаптироваться к изменениям в методе проведения атаки (после получения соответствующего оповещения); автоматизировать сбор данных, рассылку оповещений и ответы на интересующие объекты; а также изменить конфигурацию в соответствии с рабочими процессами клиента.
- **Непрерывность:** при обнаружении событий атак постоянно работающие коллекторы активируют триггеры, оповещая пользователей и их системы о появлении злоумышленных действий, включенных в список наблюдения.

Организациям, уделяющим достаточное внимание обеспечению собственной безопасности, сегодня приходится иметь дело с очень быстро меняющейся картиной угроз. Темпы создания и распространения атак неумолимо растут. Появляются «дизайнерские» атаки, направленные на отдельные организации. Для проведения таких атак злоумышленники используют целенаправленно собранную информацию, позволяющую повысить эффективность атаки и свести к минимуму риск обнаружения. Участились случаи взлома технологий упреждающей защиты. Поэтому у предусмотрительных организаций появился спрос на простые в использовании, комплексные средства защиты, с помощью которых можно более точно обнаруживать присутствие злоумышленников, а после обнаружения быстро проводить расследование и вносить необходимые исправления. Лучшие решения для обнаружения угроз и реагирования на инциденты обеспечивают повышенный уровень эффективности защиты даже тогда, когда из-за увеличения количества систем им приходится обрабатывать все большее и большее количество информации. Решение McAfee® Active Response оснащено превосходными функциями, не требующими предварительной настройки, способно автоматически обмениваться данными с уже имеющимися решениями для управления безопасностью и предусматривает возможность индивидуальной настройки в соответствии с предпочтениями пользователя. Благодаря этим особенностям оно значительно сужает возможности злоумышленников по нанесению ущерба вычислительным активам и корпоративному бренду атакуемой компании.

Меняющаяся картина угроз

На сегодняшний день у крупных компаний уже есть понимание того, что нарушение безопасности может произойти в любой момент и что они должны быть готовы эффективно противостоять попыткам взлома. Для этого необходимо выявлять атаки на раннем этапе, обнаруживать текущие действия и распознавать признаки атаки (ПА). Вместе с пониманием этого факта приходит осознание того, что для устранения имеющихся пробелов с точки зрения сбора информации, обнаружения атак, выявления угроз и реагирования на инциденты необходимы новые технологии.

intel Security

Поддерживаемые платформы

- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2; Windows 7, 8, 8.1, 10
- Linux (Red Hat, CentOS, SUSE, Ubuntu)

Ограничения используемых в настоящее время подходов к реагированию на инциденты

Выполняя задачу расследования предполагаемого или уже известного инцидента в рамках всей организации, специалисты по реагированию на инциденты и администраторы систем безопасности, как правило, сталкиваются с двумя основными ограничительными факторами: временем и масштабом. Имеющиеся в организации системы и средства защиты накапливают большое количество подробной информации, но для сбора и анализа этой информации необходимо очень много времени. Поскольку при сборе данных скорость играет критически важную роль, организациям приходится идти на серьезные компромиссы в том, что касается характера собираемых данных и количества систем, с которых эти данные собираются. Кроме того, объем собираемых данных, подлежащих фильтрации для выявления важной информации, настолько велик, что обрабатывать его становится все труднее и труднее.

Что касается средств реагирования на инциденты, то чаще всего это сценарии, написанные самими специалистами по реагированию на инциденты. С их помощью осуществляется сбор основного массива данных, используемых впоследствии для более широкого анализа. Это полноценный набор данных и средств работы с данными, но если говорить об изменении масштаба и скорости, то его возможности ограничены. Отсутствие возможности проводить прямое расследование по конкретным ПА в пределах всей организации зачастую вынуждает специалистов по реагированию на инциденты проявлять близорукость в работе по обнаружению угроз и реагированию на инциденты. Как правило, такая работа бывает искусственно ограничена заданными временными рамками, и это может приводить к значительным упущениям в процессе реагирования на инциденты. По сути, эти серьезные затруднения в работе специалистов искусственно вызваны теми ограничениями, которые имеются у используемых ими в настоящее время средств реагирования на инциденты.

Комплексное средство обнаружения угроз и реагирования на инциденты для защиты конечных точек

Решение McAfee Active Response позволяет непрерывно обнаруживать сложные угрозы безопасности и реагировать на них. С его помощью специалисты-практики могут отслеживать уровень безопасности, повышать качество обнаружения угроз и расширять возможности реагирования на инциденты благодаря наличию функций опережающего обнаружения угроз, подробного анализа инцидентов, проведения компьютерно-технической экспертизы, генерирования комплексных отчетов, рассылки приоритетных оповещений и принятия приоритетных мер. В McAfee Active Response, оптимизированном для удовлетворения строгих критериев обнаружения угроз и реагирования на инциденты на конечных точках (endpoint detection and response — EDR), используются предопределенные и настраиваемые пользователем коллекторы, позволяющие осуществлять детальный поиск информации во всех системах. Целью поиска является обнаружение признаков не только таких атак, которые присутствуют в виде запущенных процессов, но и таких, которые на данный момент бездействуют или уже удалены. Более того, McAfee Active Response дает пользователям возможность не только осуществлять поиск по ПА, имеющим место в настоящее время, но создавать триггеры, которые будут срабатывать при обнаружении того или иного ПА в будущем. Триггеры позволяют рассылать заранее заданные оповещения и принимать заранее определенные меры в соответствии с поставленными задачами по обеспечению безопасности.

Решение McAfee Active Response наглядно демонстрирует эффективность архитектуры Security Connected. Оно дает возможность непрерывно собирать информацию о происходящем на конечных точках, что позволяет быстрее выявлять случаи нарушения безопасности. Кроме того, оно предоставляет специалистам необходимый инструментарий для более быстрого устранения возникающих проблем оптимальным для компании образом.

Управление всем этим многообразием функций осуществляется посредством программного обеспечения McAfee® ePolicy Orchestrator® (McAfee ePO™) через уровень обмена данными McAfee (McAfee Data Exchange Layer). Это дает возможность централизованно обеспечить масштабируемость и расширяемость данного решения без необходимости привлекать для администрирования продукта дополнительных сотрудников.

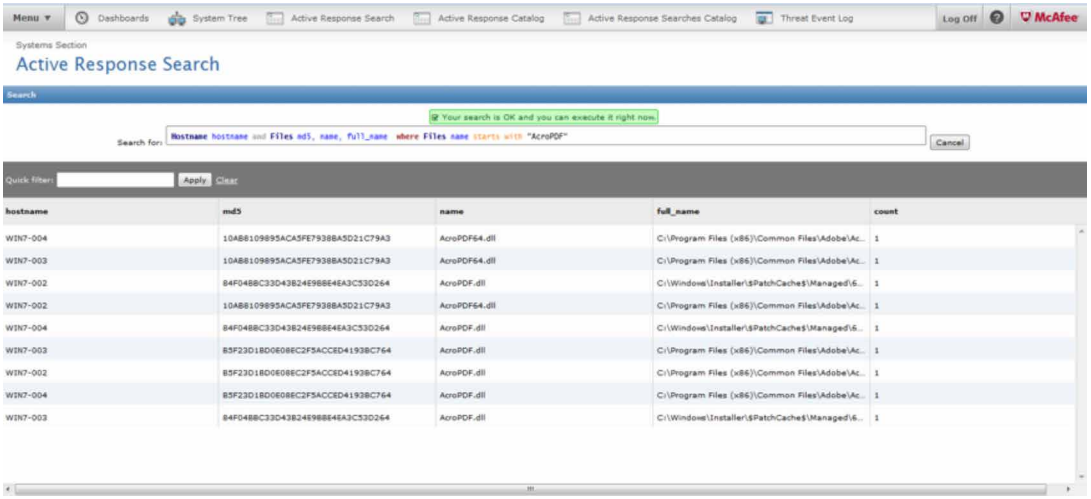

Рис. 1. Пользовательский интерфейс поиска в McAfee Active Response

Функция	Преимущество	Преимущества для клиентов	Дифференциация
Коллекторы	Коллекторы дают пользователям возможность находить и визуализировать данные, содержащиеся в имеющихся системах.	Коллекторы позволяют искать информацию с целью получения подробных сведений о системах. Они позволяют выявлять потенциальные случаи критически важных нарушений безопасности или атак и дают возможность собирать и визуализировать данные с таких систем. Используя любой из нескольких распространенных языков сценариев, пользователи могут легко настраивать свои собственные коллекторы и ответы, что позволяет достичь оптимального уровня конфигурируемости и адаптируемости.	McAfee Active Response проверяет не только исполняемые и запущенные файлы, но и такой код, который на данный момент бездействует или который был удален в попытке скрыть следы злоумышленника. McAfee Active Response может осуществлять поиск по файлам, сетевому потоку, реестру и процессам.
Триггеры	Триггеры дают специалисту по безопасности возможность непрерывно отслеживать критически важные изменения в событиях и состояниях как в настоящем, так и в будущем с помощью одного набора инструкций.	Действия инициируются заранее установленным триггером, в результате срабатывания которого генерируется событие или выполняется ответ. McAfee Active Response идет дальше статических, «застывших» представлений и дает возможность принимать меры реагирования в непрерывном режиме.	Наблюдая угрозы, имеющие место в настоящем, McAfee Active Response может устанавливать триггеры для запуска ответов на угрозы, которые могут появиться в будущем.

Функция	Преимущество	Преимущества для клиентов	Дифференциация
Реакции	Реакции представляют собой заранее заданные и настраиваемые действия, запускаемые при выполнении условий триггера. Они дают возможность выслеживать и устранять угрозы.	Реакции дают пользователям возможность выполнять такие действия как, например, поиск удаленных из системы файлов по хэшу файла (MD5 и SHA1); проверка на наличие узлов, активно подключенных или подключавшихся к тому или иному IP-адресу; поиск вредоносного файла (не в формате PE), который не был открыт и не «сдетонировал» в системе (например, поиск вредоносного PDF-файла, скопированного в файловую систему, но не открытого).	McAfee Active Response настроен на выполнение определенных действий в зависимости от результатов поиска и дает пользователю возможность настраивать дополнительные действия для решений особых задач.
Централизованное управление с помощью программного обеспечения McAfee ePO	Наличие в среде одной-единственной консоли управления позволяет реализовать комплексный подход к управлению и автоматизации.	Администраторы могут использовать программное обеспечение McAfee ePO в рамках архитектуры Security Connected для создания автоматических ответов на триггеры и результаты поиска, а также для реагирования на инциденты и для устранения угроз. Управление с помощью одной-единственной панели позволяет собирать больше информации об уровне защищенности организации без создания дополнительной административной нагрузки. Это упрощает оперативные аспекты и сокращает временные затраты административного персонала.	Возможность управлять и принимать меры посредством одной-единственной консоли является неоспоримым конкурентным преимуществом. Использование одной-единственной консоли дает нам уникальную возможность обеспечивать защиту разных платформ с помощью полнофункционального набора средств защиты, в который входит и McAfee Active Response.
Security Connected	Упрощает обмен данными с другими продуктами компании McAfee (входящей в состав Intel Security) через уровень обмена данными (DXL).	Благодаря предлагаемым данной платформой инновационным концепциям, оптимизированным процессам и практическим рекомендациям, интеграция с Security Connected дает возможность понизить уровень риска, сократить время реагирования на инциденты и снизить расходы на администрирование и обслуживающий персонал.	

Дополнительную информацию о преимуществах McAfee Active Response можно получить по адресу **www.mcafee.com/ru/about/active-response-technology-preview.aspx**.

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной»,
Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com