Три глобальные проблемы информационной безопасности или зачем нужна система адаптивной безопасности

В настоящее время в мире ИТ наблюдается несколько глобальных трендов, которые влияют на развитие ИБ.

Первый тренд – это дигитализация бизнеса и переход к концепции клиент-облако. Бизнес все больше систем и приложений переводит в облачные платформы, предоставляет доступ внутренним работникам, удаленным пользователям, контракторам и партнерам к своим ресурсам с различных устройств – ПК, смартфонов, планшетов. Все это приводит к усложнению задачи по обеспечению должного уровня безопасности.

Второй тренд – это увеличение сложности атак и времени, необходимое для их обнаружения и устранения. Согласно исследованиям «Ponemon Institute» среднее время обнаружения атаки в 2015 году в финансовых учреждениях составляло 98 дней (!), а в розничных сетях – более полугода (197 дней). В течение данного времени вредоносные программы получают доступ к различным ресурсам компании, воруют данные и передают их преступным кибер-группировкам. Проблема усугубляется еще и тем, что после обнаружения атаки проходит длительное время на расследование причиненного ущерба и его устранения. Это занимает времени от несколько недель до нескольких месяцев. В виде примера можно вспомнить историю с SONY Pictures, когда злоумышленники похитили более 100 ТВ данных, включая 5 новых фильмов, всю почтовую переписку, медицинские и персональные данные актеров, бухгалтерию и после удалили всю информацию с серверов и рабочих станций. Восстановление работоспособности компании заняло более 6 месяцев.

Третий тренд – это острая нехватка специалистов по информационной безопасности. Согласно данным, опубликованным ISACA в 2015 году, штат отдела ИБ не был укомплектован в 62% организаций. То есть специалисты отдела безопасности перегружены и просто не успевают выполнять свои прямые обязанности – обнаруживать и устранять атаки. С учетом того, что бюджеты на информационную безопасность уменьшаются, можно сказать, что большинство организаций не готовы к обеспечению должного уровня безопасности и противостоянию современным видам целенаправленных атак.

Выход из сложившейся ситуации компания Intel Security видит в изменении подхода к ИБ и переходу к архитектуре адаптивной безопасности.

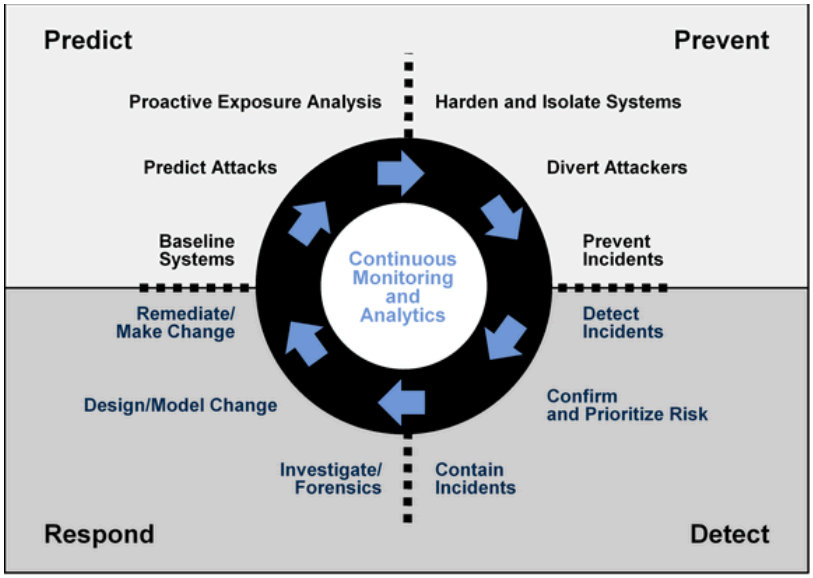
В 2014 году аналитическое агентство Gartner выпустило документ «Создание Адаптивной Архитектуры Безопасности для защиты от целенаправленных атак». В данном документе обозначены основные проблемы в области ИБ и рекомендации. Итак, основные проблемы:

- Существующих технологий защиты недостаточно для противостояния современным целенаправленным атакам.
- Большинство организаций до сих пор инвестируют средства только в технологии защиты.
- Технологии защиты, предотвращения атак, детектирования и расследования/устранения от различных производителей не интегрированы друг с другом, что приводит к дополнительному хаосу, увеличивает затраты и снижает эффективность ИБ.
- ИБ не хватает постоянной видимости происходящего для детектирования целенаправленных атак.
- Корпоративные системы находятся под постоянными и не прекращающимися атаками, поэтому понятие «Incident Response» больше не подходит.

Рекомендации от Gartner:

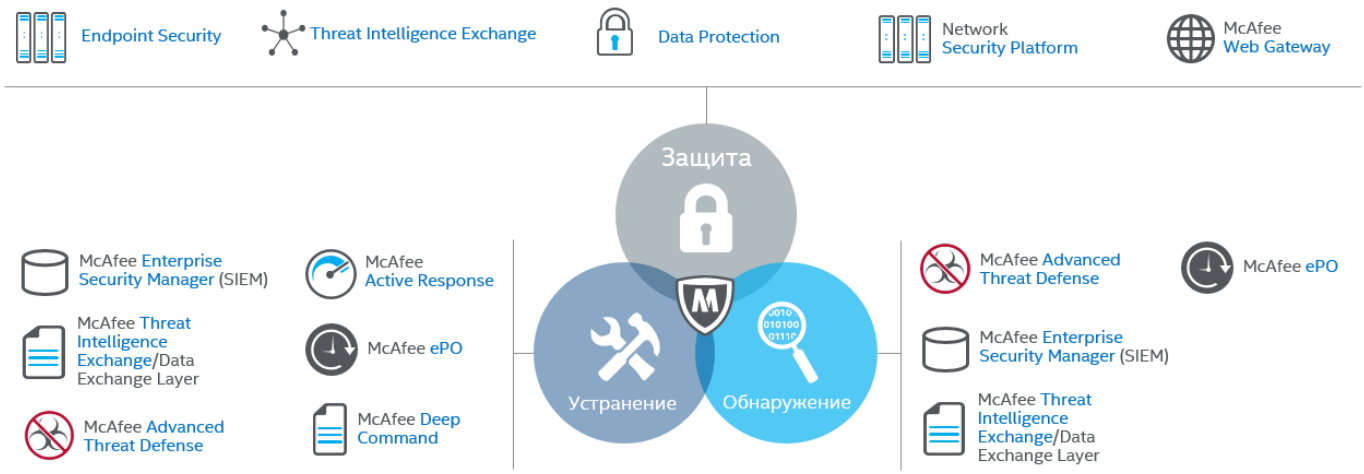
- Поменять понятие «Incident Response» на «Continuous Response», где предполагается, что системы постоянно скомпрометированы и им необходим непрерывный мониторинг и восстановление.
- Создание Адаптивной Архитектуры Безопасности для защиты от целенаправленных атак, используя 12 критических функций от Gartner.
- Направить больше инвестиции на системы обнаружения и быстрого реагирования, и уменьшить на защиту и предотвращение.
- Отдавать предпочтения производителям, которые предлагают контекстно-ориентированные платформы для сетевой безопасности, безопасности рабочих станций и приложений, а также интегрированный подход к анализу, предотвращению, обнаружению и реагированию на атаки.
- Развивать Security Operation Center (SOC), который позволяет осуществлять постоянный мониторинг и предотвращение атак.
- Осуществлять полный мониторинг на всех уровнях ИТ: сетевых пакетов, сетевых потоков, активности ОС, контента, поведения пользователей.

12 Критических функций и 4 основные области приведены на рисунке ниже.



Основные 4 области: Prevent (Предотвращение), Detect (Обнаружение), Respond (Реакция, ответ) и Predict (Предсказание). В центре – непрерывный мониторинг и анализ.

Компания Intel Security, один из ведущих игроков рынка ИБ, строго следуя рекомендациям агентства Gartner представляет на рынке законченную и работающую Архитектуру Адаптивной Безопасности с концепцией Protect, Detect, Correct (Защита, Обнаружение, Устранение).



Решения по Защите (Protect) представлены следующими продуктами:

- защита конечных точек и серверов, **McAfee Endpoint Security** и **McAfee Server Security**. Находятся в квадранте лидеров Gartner на протяжении последних 13 лет.
- контроль запуска приложений и изменений файлов, **McAfee Application and Change Control**, для критичных и специализированных серверов.
- защита виртуальных сред, **McAfee MOVE-AV**.
- сетевые системы обнаружения и предотвращения вторжений, **McAfee Network Security Platform**, с производительностью от 100 Мбит/с до 320 Гбит/с. Находятся в квадранте лидеров Gartner на протяжении последних 9 лет.
- шлюз веб фильтрации с контентным анализом данных, **McAfee Web Gateway**. Находился в квадранте лидеров Gartner на протяжении 5 лет, последние два года – в квадранте провидцев Gartner.
- системы предотвращения утечек данных, **McAfee Data Loss Prevention**, и шифрования данных, **McAfee Complete Data Protection**. Находятся в квадранте лидеров Gartner на протяжении последних 7 и 8 лет соответственно.

Решения для Обнаружения (Detect) представлены следующими продуктами:

- центральная консоль управления, **McAfee ePolicy Orchestrator**.
- система SIEM, **McAfee Enterprise Security Manager (ESM)**, является самой быстродействующей SIEM по признанию Gartner. Находится в квадранте лидеров Gartner на протяжении последних 6 лет. Основной элемент архитектуры для непрерывного мониторинга.
- **McAfee Threat Intelligence Exchange (TIE)** – локальная база данных для сбора и обмена

информацией о существующих угрозах в компании. Уникальность данного решения заключается в том, что собирается информация о репутации запускаемых файлов в компании, также существует возможность подключить дополнительные источники репутаций, таких как **VirusTotal**, **NorSec**, **McAfee GTI** и другие. Обмениваться информацией об угрозах могут элементы безопасности и других производителей, поддерживающих шину обмена данными **DXL** – **Data Exchange Layer**.

- **McAfee Advance Threat Defense (ATD)** – устройство класса «песочница» для определения репутации файлов и их класса. Для исследования файлов применяется как динамический (запуск файла в защищенной виртуальной среде), так и статический анализы кода, что позволяет эффективно обнаруживать атаки с отложенным запуском или системой определения «песочниц».

Решения для Устранения (Correct) представлены теми же решениями, что и для Обнаружения, и дополнительными продуктами:

- **McAfee Active Response (MAR)** – инструмент для активных действий класса EDR (Endpoint Detection and Response). Позволяет автоматизировать получение информации в режиме реального времени о состоянии систем и их изменениях, что можно классифицировать, как индикаторы атак (IoC). Также позволяет производить поиск информации по заданным запросам, например, поиск удаленных файлов по хешу, проверка рабочих станций, подключавшихся к определенному IP адресу, установленные агенты и обновления безопасности. Также позволяет удалять обнаруженные вредоносные файлы и возвращать систему к ее первоначальному состоянию.

Сценарий использования

Как же на практике может работать система адаптивной безопасности от Intel Security? Давайте рассмотрим пример, где злоумышленник решил атаковать компанию «ААА», применив социальную инженерию и создав вредоносный файл специально для атаки на данную компанию. Злоумышленник, проведя подготовительную работу, в LinkedIn или в Facebook нашел профайлы администраторов баз данных компании «ААА», посмотрел в каких сообществах или группах они состоят, какие дискуссии ведут, и выяснил, что компания «ААА» использует базы данных Oracle. Злоумышленник присылает письмо на адрес администратора, где объясняет, что они состоят в одной группе на LinkedIn и его тоже интересуют вопросы оптимизации запросов. Он предлагает скачать по ссылке инструкцию по оптимизации. Администратор по ссылке скачивает PDF файл и открывает его…

McAfee Web Gateway проверяет скачиваемый файл, не находит в нем ничего подозрительного и через шину **DXL** запрашивает репутацию данного файла у **McAfee Threat Intelligence Exchange**. Так как файл совершенно новый, то репутации у него нет. **TIE** запрашивает репутацию у третьих источников – **McAfee GTI** и VirusTotal, но и там репутации данного файла тоже нет. **TIE** сообщает полученную информацию **McAfee Web Gateway** и он, согласно заданным политикам, может удалить файл, не имеющий репутации, но, так как в компании «ААА» используется **McAfee Advanced Threat Defense**, файл отправляется на проверку в «песочницу». При проверке файла выясняется, что он содержит скрипт для скачивания дополнительных файлов, таких как *keylog.exe* и *killdisk.exe*. **ATD** обновляет репутацию файла в **TIE** на «известный плохой», собирает индикаторы атаки (IP адрес, адрес электронной почты, домен, хеш файла и пр.) и автоматически пересылает их в **McAfee Enterprise Security Manager**. В это время **TIE** через **DXL** оповещает остальные компоненты безопасности. **McAfee Endpoint Security** автоматически переводит рабочую станцию администратора в режим карантина, удаляет вредоносный файл и может запустить сканирование жесткого диска. Агент **DLP** переводится в режим усиленных политик безопасности. Сетевой IPS **McAfee Network Security Platform** обновляет политики, поместив IP адрес в черный список, **Web Gateway** также заносит IP адрес в черный список. **ESM** выдает

оповещение администратору безопасности о заблокированной атаке. Администратор при помощи **McAfee Active Response** запускает поиск файла по хешу. Данный файл обнаружен еще на 2 машинах в электронной почте. Файл еще не открывали, поэтому никакой подозрительной активности зафиксировано не было. Администратор дает команду удалить данные файлы. Файлы удалены, атака отражена. От скачивания файла до полного обезвреживания прошло всего пару минут. **ESM** дополнительно проверяет исторические логи, чтобы убедиться, что у других рабочих станций не было контактов с этим вредоносным IP адресом и доменом.

Итак, какие преимущества дает Архитектура Адаптивной Безопасности?

1. Время реакции на инциденты – секунды от обнаружения до восстановления системы.
2. Автоматизация – автоматическое блокирование вредоносных файлов, IP адресов, доменов и обновление политик решений ИБ в соответствии с ситуацией. Все элементы ИБ работают как единое интегрированное решение, что в разы повышает эффективность всей системы и понижает показатели совокупной стоимости владения (TCO) отдела безопасности.
3. Освобождение администраторов от ручного анализа и работы, что позволяет им заниматься другими необходимыми работами или повышением квалификации.
4. Возможность интегрировать в архитектуру решения других производителей, которые поддерживают шину DXL – CyberArk, Rapid7, ForcePoint, Brocade, Avecto, Titus и других.

Представленная архитектура уже реализована и успешно работает в разных компаниях, помогая снижать затраты и увеличивать эффективность работы отдела ИБ.

Более подробную информацию можно найти на сайте www.mcafee.com или у партнеров Intel Security.

Об авторе

Руслан Барбашин, консультант по информационной безопасности / аккаунт менеджер – Центральная Азия, Кавказ, Украина и Беларусь, Intel Security Group

ruslans.barbasins@intel.com | https://www.linkedin.com/in/ruslansbarbasins