План освоения облака AWS

Перспектива безопасности

Июнь 2016 г.

Уведомления

Этот документ предоставляется исключительно в информационных целях. В нем представлены текущие предложения продуктов и практики AWS, актуальные на дату публикации, которые могут меняться без предварительного уведомления. Клиентам необходимо провести собственную независимую оценку представленной в документе информации и вариантов использования продуктов и услуг AWS. Указанные информация, продукты и услуги предоставляются «как есть», без какой-либо явной или подразумеваемой гарантии. Данный документ не создает никаких гарантий, контрактных обязательств и иных обязательств, условий или заверений от AWS, ее дочерних организаций, поставщиков или лицензиатов. Обязанности и финансовые обязательства AWS в отношении клиентов компании регулируются соглашениями AWS. Данный документ не является таким соглашением, а также не вносит изменения в какие-либо соглашения, заключенные между компанией AWS и ее клиентами.

Содержание

Резюме 4

Введение 4

Преимущества AWS в сфере безопасности 6

Проектирование с учетом безопасности 7

Высокая степень автоматизации 7

Высокая доступность 8

Высокая степень доверия 8

Директивный компонент 9

Несколько важных моментов 11

Профилактический компонент 12

Несколько важных моментов 13

Компонент обнаружения 14

Несколько важных моментов 15

Реагирующий компонент 16

Несколько важных моментов 17

Итак, в путь! Определяем стратегию 18

Несколько важных моментов 20

Итак, в путь! Составляем программу 21

Базовая пятерка 22

Дополнение к основным сценариям 24

Примеры последовательностей спринтов 26

Несколько важных моментов 28

Итак, в путь! Разработка надежных мер безопасности 29

Заключение 30

Приложение A. Отслеживание прогресса для перспективы безопасности AWS CAF 31

Ключевые факторы безопасности 31

Модель выполнения сценариев безопасности 32

Классификация и определения CAF 35
Примечания 35

Резюме

План освоения облака[1] (CAF) Amazon Web Services (AWS) содержит рекомендации по координации деятельности разных частей организации, которая выполняет переход к облачным вычислениям. Руководство CAF подразделяется на несколько направлений, связанных с внедрением облачных ИТ-систем. Эти направления называются *перспективами*, а каждая перспектива далее подразделяется на *компоненты*. Каждой из семи перспектив CAF посвящено свое техническое описание.

В этом техническом описании рассматривается перспектива безопасности, ориентированная на внедрение рекомендаций и процедур использования существующих механизмов контроля безопасности при работе с AWS в вашей среде.

Введение

Для AWS безопасность на первом месте. Все клиенты AWS пользуются всеми преимуществами центров обработки данных и сетевой архитектуры, которые разрабатывались для организаций с повышенными требованиями к безопасности. AWS и ее партнеры предлагают сотни инструментов и функций для решения следующих задач в сфере безопасности: обеспечения видимости системы, ее доступности для аудита и контроля и повышения ее гибкости. Это означает, что необходимый уровень безопасности можно обеспечить без серьезных капитальных вложений и с гораздо более низкими операционными затратамипо сравнению с локальной средой.

Рис. 1. Перспектива безопасности AWS CAF

Цель перспективы безопасности – помочь вам структурировать выбор и внедрение механизмов контроля, которые подходят вашей организации. Как показано на рисунке 1, компоненты перспективы безопасности структурируют принципы, на основе которых будет преобразована культура безопасности вашей организации. В этом техническом описании рассматриваются возможные меры для каждого компонента и инструменты оценки прогресса:

- **Директивные** механизмы контроля устанавливают модели управления, оценки рисков и соответствия требованиям, согласно которым будет функционировать новая среда безопасности.
- **Профилактические** механизмы контроля защищают ваши рабочие нагрузки и уменьшают угрозы и уязвимости.
- Механизмы контроля **обнаружения** обеспечивают полную видимость и прозрачность функционирования ваших развертываний в AWS.
- **Средства реагирования** позволяют не допустить возможных отклонений от ваших требований безопасности.

Все мы знакомы с концепцией безопасности в облаке. Тем не менее, повышение гибкости и способность действовать быстрее, в больших масштабах и с меньшими затратами не отменяют общепринятые принципы информационной безопасности.

После обзора четырех компонентов перспективы безопасности мы переходим к описанию мер, которые можно предпринять на пути к облаку, чтобы обеспечить полную безопасность вашей среды.

- Определите **стратегию безопасности** в облаке. В самом начале пути необходимо оценить бизнес-цели вашей организации, ее подход к управлению рисками и возможности, которые ей сулит переход к облаку.

- Составьте **программу безопасности** по разработке и внедрению функций безопасности, конфиденциальности, соответствия требованиям и управления рисками. Сначала объем работ может представляться вам слишком большим, поэтому важно создать структуру, позволяющую организации решать задачи безопасности в облаке комплексно. В реализацию необходимо заложить возможность итеративной разработки, чтобы по мере развития программ совершенствовались и ваши функциональные возможности. В этом случае компонент безопасности сможет стать катализатором освоения облачных технологий в остальных частях организации.
- Разработайте надежные функциональные возможности для принятия **мер безопасности** и механизмы их совершенствования. Обеспечение безопасности – это долгий путь. Рекомендуем сделать создание новых возможностей частью операционной рутины, чтобы в результате постоянного повторения обеспечить непрерывное совершенствование.

Преимущества AWS в сфере безопасности

Безопасность облака является главным приоритетом для AWS. Став клиентом AWS, вы будете пользоваться всеми преимуществами центров обработки данных и сетевой архитектуры, которые разрабатывались для организаций с повышенными требованиями к безопасности.

Одно из преимуществ облака AWS заключается в том, что клиенты могут масштабировать свою систему и реализовывать инновации, сохраняя высокий уровень безопасности среды. Клиенты платят только за те сервисы, которые используют. Это означает, что необходимую безопасность можно обеспечить без предварительных затрат и по более низкой цене, чем в локальной среде.

В этом разделе рассматриваются преимущества платформы AWS в сфере безопасности.

Проектирование с учетом безопасности

Инфраструктура облака AWS используется в центрах обработки данных AWS и позволяет удовлетворить самые жесткие требования наших клиентов к безопасности. Инфраструктура AWS была разработана для того, чтобы обеспечить высокую доступность систем и одновременно с этим реализовать эффективные защитные механизмы, гарантирующие конфиденциальность клиентов. Все данные хранятся в надежно защищенных центрах обработки данных AWS. Сетевые брандмауэры, встроенные в облако Amazon VPC, и функции брандмауэра, реализованные в интернет-приложениях, в составе AWS WAF позволяют создавать частные сети и контролировать доступ к инстансам и приложениям.

Когда вы развертываете системы в облаке AWS, компания AWS разделяет с вами ответственность за безопасность. AWS проектирует базовую инфраструктуру с учетом принципов безопасности, а для развертываемых в AWS рабочих нагрузок клиенты могут воспользоваться собственной архитектурой безопасности.

Высокая степень автоматизации

AWS создает специализированные средства безопасности и адаптирует их с учетом уникальных особенностей среды, масштаба и глобальных требований. Создание средств безопасности с нуля позволяет AWS автоматизировать многие рутинные задачи, на которые обычно приходится тратить время экспертам по безопасности. Это означает, что эксперты по безопасности AWS могут уделять время реализации мер по повышению безопасности вашей облачной среды AWS. Кроме того, клиенты автоматизируют проектирование и эксплуатацию систем безопасности, используя полный набор соответствующих API и инструментов. Управление идентификацией, сетевую безопасность и защиту данных, а также функции мониторинга можно полностью автоматизировать и реализовывать с помощью распространенных методов разработки программного обеспечения, которыми вы уже пользуетесь. Клиенты предпочитают автоматизировать реагирование на проблемы безопасности. Если автоматизация выполнена с помощью сервисов AWS, то вашим специалистам не нужно отслеживать состояние безопасности и реагировать на события – система самостоятельно осуществляет мониторинг, анализ ситуации и инициирует отклик.

Высокая доступность

AWS строит центры обработки данных в разных географических регионах. Отказоустойчивость обеспечивается наличием в каждом из регионов нескольких зон доступности. AWS проектирует центры обработки данных с избыточной пропускной способностью, чтобы в случае серьезного сбоя было достаточно ресурсов для балансировки нагрузки трафика и маршрутизации трафика на исправные объекты. Это позволяет свести к минимуму последствия сбоев для клиентов. Клиенты также применяют эту стратегию (используют несколько зон доступности в нескольких регионах) для создания отказоустойчивых приложений по сенсационно низкой цене, для удобной репликации и резервного копирования данных, а также для последовательного развертывания глобальных механизмов контроля безопасности в масштабах всего бизнеса.

Высокая степень доверия

Среды AWS непрерывно проходят проверки и получают сертификаты от агентств по аккредитации из разных стран мира. Это означает, что часть актуальных для вас задач по обеспечению соответствия требованиям уже выполнена. Дополнительные сведения о требованиях и стандартах безопасности, которые соблюдает AWS, см. на веб-странице Соответствие требованиям облака AWS[2]. Чтобы помочь вам в соблюдении конкретных государственных, отраслевых и корпоративных требований и стандартов безопасности, AWS предоставляет сертификационные отчеты, в которых подтверждается соответствие облачной инфраструктуры AWS требованиям большого числа международных стандартов безопасности. Для получения доступных отчетов о соответствии требованиям обратитесь к своему представителю по обслуживанию аккаунтов AWS. Клиенты включают множество обслуживаемых AWS механизмов контроля в собственные программы соответствия требованиям и сертификации, что не только устраняет необходимость в самостоятельном обслуживании этих механизмов, но и позволяет снизить затраты на поддержку системы и выполнение мер обеспечения безопасности. Имея надежный фундамент, вы легко сможете оптимизировать безопасность своих рабочих нагрузок с учетом требований гибкости, отказоустойчивости и масштабирования.

Далее в этом техническом описании будут представлены все компоненты перспективы безопасности. С помощью этих компонентов вы сможете выделить задачи в области безопасности, решение которых поможет успешно перейти к облаку.

Директивный компонент

Директивный компонент перспективы безопасности AWS содержит рекомендации по планированию стратегии безопасности при переходе к AWS. Залог эффективного планирования – четко определить, какие инструкции будут предоставлены специалистам, которые создают и эксплуатируют вашу среду безопасности. Эта информация должна содержать достаточно подробные инструкции, позволяющие определить, какие требуются механизмы контроля и как их следует использовать. Сферы, которые необходимо учитывать в первую очередь:

- **Управление аккаунтами**: организация должна внедрить процессы и процедуры управления аккаунтами AWS. Необходимо определить, как будут собираться и обслуживаться инвентарные данные об аккаунтах, какие соглашения и изменения их регулируют и какие критерии использовать для выбора нужного времени создания аккаунта AWS. Организация должна разработать единообразную процедуру создания аккаунтов, позволяющую гарантировать правильность первоначальных настроек и однозначность владения.
- **Владение аккаунтами и контактная информация**: необходимо внедрить подходящую модель управления аккаунтами AWS, которая будет использоваться в организации повсеместно, и спланировать обслуживание контактной информации для каждого аккаунта. Целесообразно создавать аккаунты AWS, привязанные к спискам электронной рассылки, а не отдельным адресам электронной почты. Это позволит группе пользователей отслеживать сведения от AWS об истории вашего аккаунта и реагировать на них. Кроме того, такой подход обеспечит устойчивость системы в случае внутренних кадровых перестановок, поскольку позволяет назначать ответственность за безопасность. Укажите специалистов по безопасности в качестве контактной точки по вопросам безопасности, чтобы ускорить срочный обмен информацией.

- **Система контроля**: внедрите и используйте соответствующую отраслевым стандартам систему контроля; установите, требуются ли какие-либо изменения или дополнения, чтобы использовать сервисы AWS на ожидаемом уровне безопасности. Выполните пробное сопоставление соответствия требованиям, чтобы установить, как использование сервисов AWS отразится в требованиях соответствия и механизмах контроля безопасности.
- **Владение механизмами контроля**: изучите информацию о модели общей ответственности AWS[3] на веб-сайте AWS, чтобы установить, нужно ли внести изменения в систему владения механизмами контроля. Проанализируйте и обновите матрицу распределения ответственности (схему RACI), чтобы добавить в нее информацию о владении механизмами контроля, которые используются в среде AWS.
- **Классификация данных**: изучите существующие классификации данных и определите, как будет осуществляться управление этими классификациями в среде AWS и какие механизмы контроля целесообразно использовать.
- **Управление изменениями и активами**: определите, как в AWS будет осуществляться управление изменениями и управление активами. Создайте средства, позволяющие определить, какие активы существуют, для чего используются системы и как наладить безопасное управление этими системами. Эти средства можно интегрировать в существующую базу данных управления конфигурациями (CMDB). Оцените целесообразность введения практики именования и добавления тегов, которая позволит выполнять идентификацию и управление на требуемом уровне безопасности. Этот подход можно использовать для определения и отслеживания метаданных, используемых для идентификации и контроля.

- **Местоположение данных**: проверьте критерии возможного расположения данных, чтобы определить, какие механизмы контроля потребуются для управления конфигурацией и использованием сервисов AWS в регионах. Клиенты AWS выбирают регион (регионы) для размещения своего контента. Это позволяет заказчикам, у которых есть требования к территориальному размещению, создавать среды в выбранных местоположениях. Заказчики могут выполнять репликацию и резервное копирование контента в несколько регионов, но AWS перемещает и реплицирует контент заказчиков только в регион или регионы, выбранные заказчиками.

- **Доступ по принципу минимальных полномочий**: создайте культуру безопасности организации, основанную на принципе минимальных полномочий и строгой аутентификации. Внедрите протоколы для защиты доступа к конфиденциальным учетным данным и ключевым материалам, связанным с каждым аккаунтом AWS. Сформулируйте ожидания в отношении способов делегирования полномочий разработчикам ПО, операторам и другим сотрудникам, участвующим во внедрении облака.

- **Меры безопасности: сценарии и перечни задач**: определите шаблоны безопасности, на основе которых будут созданы диапазоны допустимых показателей для использования организацией в качестве ориентиров в долгосрочной перспективе. Реализуйте эти сценарии в качестве автоматизированных перечней задач; документируйте любые вмешательства специалистов в процесс должным образом.

Несколько важных моментов

- **Создайте** специализированную модель общей ответственности AWS для своей экосистемы.
- **Используйте** строгую аутентификацию в рамках схемы защиты для всех пользователей в вашей учетной записи.
- **Пропагандируйте** культуру ответственности за безопасность среди групп специалистов, работающих с приложениями.
- **Расширяйте** свою модель классификации данных, включая в нее сервисы в AWS.

- **Интегрируйте** цели и рабочие функции команд специалистов, ответственных за разработку, эксплуатацию и безопасность.
- **Оцените** целесообразность разработки стратегии именования и отслеживания аккаунтов, используемых для управления сервисами в AWS.
- **Централизуйте** списки рассылок по телефону и электронной почте, чтобы можно было отслеживать деятельность рабочих групп.

Профилактический компонент

Профилактический компонент перспективы безопасности AWS содержит рекомендации по внедрению инфраструктуры безопасности в среде AWS и в вашей организации. Ключ к внедрению подходящего набора механизмов контроля заключается в создании условий для специалистов по безопасности вашей организации, в которых они смогут обрести уверенность и развить навыки автоматизации и развертывания, необходимые для защиты организации в гибкой и масштабируемой среде, то есть AWS.

Используйте директивный компонент, чтобы определить, какие потребуются механизмы контроля и инструкции, а затем с помощью профилактического компонента определите, как эффективно эксплуатировать механизмы контроля. AWS регулярно предоставляет инструкции и рекомендации по сценариям использования сервисов AWS и развертывания рабочих нагрузок. Эти сценарии можно использовать в качестве справочного ресурса по внедрению механизмов контроля. Посетите Центр безопасности AWS Security Center, ознакомьтесь со статьями в блоге и последними видео Security Track с саммита AWS Summit и конференции re:Invent.

Проанализируйте следующие области, чтобы определить, какие изменения (если применимо) нужно внести в существующую архитектуру безопасности и действующие практики безопасности. Это позволит плавно и в соответствии с планом реализовать стратегию освоения AWS.

- **Идентификация и доступ**: интегрируйте использование AWS в жизненный цикл рабочих ресурсов организации и в системы аутентификации и авторизации. Четко и подробно сформулируйте политики и обозначьте роли, связанные с соответствующими пользователями и группами. Установите диапазоны допустимых значений, позволяющие вносить важные изменения исключительно автоматическими методами, блокирующие нежелательные изменения и автоматически выполняющие их откат. Это ограничит доступ человека к производственным системам и данным.
- **Защита инфраструктуры**: разработайте так называемый «базовый уровень безопасности», включающий границы доверия, конфигурацию и принципы обслуживания системы безопасности (например, укрепление и внесение исправлений) и другие подобающие точки принудительной реализации политик (например, группы безопасности, AWS WAF, Amazon API Gateway), чтобы удовлетворить потребности, выявленные с помощью директивного компонента.
- **Защита данных**: используйте подобающие защитные механизмы для обеспечения безопасности переносимых и хранимых данных. К числу таких механизмов безопасности можно отнести механизмы точного контроля доступа к объектам, создание и контроль ключей шифрования, используемых для шифрования данных, выбор подходящих методов шифрования и токенизации, проверку целостности и подобающие способы хранения данных.

Несколько важных моментов

- **Рассматривайте** безопасность как код, который не только позволяет развертывать и проверять инфраструктуру безопасности, но и обеспечивает возможность масштабирования и гибкость для защиты организации.

- **Создавайте** диапазоны допустимых значений, разумные параметры по умолчанию и предлагайте шаблоны и передовые практики в качестве кода.
- **Создавайте** сервисы безопасности, которые организация сможет использовать для многократно выполняемых или в высшей степени конфиденциальных функций безопасности.
- **Определите** пользователей, а затем составьте подробный план их взаимодействия с сервисами AWS.
- **Используйте** инструмент AWS Trusted Advisor для непрерывной оценки состояния безопасности AWS; оцените целесообразность анализа качества архитектуры AWS.
- **Обозначьте** минимальные допустимые для нормального функционирования системы базовые показатели безопасности и непрерывно работайте над повышением планки для рабочих нагрузок, безопасность которых вы обеспечиваете.

Компонент обнаружения

Компонент обнаружения перспективы безопасности AWS CAF содержит рекомендации по обеспечению прозрачности состояния безопасности вашей организации. Сервис AWS CloudTrail (и некоторые другие), журналы сервисов и значения, возвращаемые API и интерфейсом командной строки, — это бесценный источник информации и данных. Интеграция этих источников безопасности в масштабируемую платформу для мониторинга журналов и управления ими, управления событиями, тестирования, инвентаризации и аудита обеспечит прозрачность и операционную гибкость, а это, в свою очередь, — уверенность в безопасности операций.

- **Ведение журнала и мониторинг**: AWS предоставляет встроенные механизмы ведения журналов и сервисы, которые можно использовать для обеспечения повышенной прозрачности любых событий в среде AWS практически в режиме реального времени. Эти инструменты можно интегрировать в существующие решения для ведения журналов и мониторинга. Глубокая интеграция данных, полученных из систем ведения журналов и мониторинга, в бизнес-процессы ИТ-организации обеспечит комплексное решение проблем в сфере безопасности.

- **Проверка безопасности**: проверьте среду AWS, чтобы убедиться в соблюдении установленных стандартов безопасности. Проверьте, будут ли ваши системы ожидаемым образом реагировать на определенные события, — это позволит лучше подготовиться к фактическим событиям. В качестве примера тестирования безопасности можно назвать сканирования уязвимостей и проверки на проникновение, а также намеренное внедрение ошибок с целью проверки соблюдения стандартов и реагирования механизма контроля ожидаемым образом.
- **Инвентаризация ресурсов**: наличие информации о том какие рабочие нагрузки развернуты и функционируют позволяет осуществлять мониторинг и гарантировать, что среда функционирует на ожидаемых и соответствующих стандартам безопасности уровнях управления безопасностью.
- **Обнаружение изменений**: если вы в своей работе опираетесь на определенные базовые профилактические механизмы контроля безопасности, вы должны знать, когда эти механизмы контроля изменятся. Обязательно предпринимайте меры, позволяющие определить разницу между конфигурацией безопасности и текущим состоянием.

Несколько важных моментов

- **Определите**, какие сведения о своей среде AWS необходимо зафиксировать в журнале, отслеживать и анализировать.
- **Определите**, как с использованием бизнес-возможностей существующего центра безопасности (SOC) интегрировать функции мониторинга безопасности и управления AWS в существующие практики.
- **Постоянно проводите** сканирования уязвимостей и проверки на проникновение в соответствии с процедурами AWS.

Реагирующий компонент

Реагирующий компонент перспективы безопасности AWS CAF содержит рекомендации по мерам реагирования в составе системы безопасности вашей организации. Если вы интегрируете среду AWS в существующую систему безопасности, а затем подготовите и смоделируете действия, требующие отклика, вы лучше подготовитесь, чтобы реагировать на реальные инциденты.

Благодаря автоматизации реакции на инциденты и восстановления системы и уменьшению объема работ по аварийному восстановлению специалисты по безопасности могут тратить меньше времени на реагирующие действия и больше – на расследование инцидентов и анализ корневых причин. В рамках адаптации своей системы безопасности требуется учитывать следующее:

- **Отклик на инциденты**: важными составляющими плана отклика на инцидент является сдерживание события и возвращение к заведомо правильному состоянию. Так, например, автоматизация определенных аспектов этих функций с помощью правил AWS Config и скриптов реагирования AWS Lambda позволяет масштабировать вашу реакцию со скоростью соединения с Интернетом. Изучите существующие процессы отклика на инциденты и определите, можно ли использовать автоматизированные механизмы отклика и восстановления в работе с ресурсами AWS (если да, то как) и как ими управлять. Функции центра безопасности должны быть тесно интегрированы с API AWS – в этом случае система будет реагировать максимально быстро. Это обеспечит возможность мониторинга безопасности и управление безопасностью при освоении облака AWS.
- **Моделирование отклика на инциденты безопасности**: моделируя события, вы сможете убедиться, что внедренные механизмы управления и процессы реагируют, как ожидается. Такой подход позволяет определить, в состоянии ли вы обеспечить эффективный отклик на реальный инцидент и восстановление системы после него.

- **Расследование инцидентов**: в большинстве случаев в среде AWS можно продолжать использовать существующие инструменты. Специалисты по расследованию инцидентов по достоинству оценят преимущества автоматизированного развертывания инструментов в разных регионах и возможность быстро и без проблем собирать большие объемы данных с помощью тех же надежных и масштабируемых сервисов, на основе которых построены их ключевые бизнес-приложения, включая Amazon Simple Storage Service (S3), Amazon Elastic Block Store (EBS), Amazon Kinesis, Amazon DynamoDB, Amazon Relational Database Service (RDS), Amazon RedShift и Amazon Elastic Compute Cloud (EC2).

Несколько важных моментов

- **Обновите** процессы отклика на инциденты, чтобы обеспечить распознаваемость среды AWS.
- **Используйте** сервисы в AWS, чтобы обеспечить поддержку расследования инцидентов в ваших развертываниях с помощью автоматизации и возможности выбора функций.
- **Автоматизируйте** отклик на инциденты, чтобы сделать систему отказоустойчивой и масштабируемой.
- **Используйте** сервисы в AWS для сбора и анализа данных в рамках расследования.
- **Проверьте** функцию отклика на инциденты путем моделирования откликов на инциденты безопасности.

Итак, в путь! Определяем стратегию

Проанализируйте существующую стратегию безопасности, чтобы определить, пойдут ли изменения, внесенные в рамках инициативы по освоению облака, на пользу тем или иным составляющим этой стратегии. Сопоставьте свою стратегию освоения облака AWS приемлемому для вашего бизнеса уровню риска, своему подходу к выполнению нормативных требований и достижению целей в области соответствия требованиям, а также выделенным вами объектам для защиты и способам их защиты. В таблице 1 приводится пример стратегии безопасности, содержащий набор принципов, которые сопоставляются конкретным инициативам и направлениям деятельности.

Принцип	Примеры действий
Инфраструктура как код.	Развитие навыков создания кода и автоматизации у специалистов по безопасности; переход к модели объединения разработки, обеспечения безопасности и эксплуатации (DevSecOps).
Проектирование диапазонов допустимых значений, а не «ворот».	Разработка мер, стимулирующих правильное поведение.
Использование облака для защиты облака.	Создание, эксплуатация инструментов безопасности и управление ими в облаке.
Поддержание актуальности, безопасная работа.	Использование новых функций безопасности, регулярная установка исправлений и выполнение замен.
Уменьшение использования постоянного доступа.	Создание каталога ролей; автоматизация KMI с использованием сервиса секретных вопросов.
Полная прозрачность.	Агрегирование журналов и метаданных AWS с журналами ОС и приложений.
Доступность больших объемов ценных сведений.	Использование хранилища данных безопасности с функциями бизнес-аналитики и аналитики.
Масштабируемый отклик на инциденты.	Обновление стандартной процедуры (SOP) отклика на инциденты и расследований с учетом принципов общей ответственности.
Самостоятельное восстановление системы.	Автоматическое исправление ошибок и восстановление заведомо правильного состояния.

Таблица 1. Пример стратегии безопасности

По мере развития вашей стратегии вы, вероятно, захотите внести изменения в сторонние системы контроля и требования организации к безопасности, а также внедрить их в систему управления рисками, которая в конечном счете позволит перейти к работе с AWS. Рекомендуется вносить изменения в принятые стандарты соответствия требованиям по мере того, как вы все лучше понимаете потребности ваших рабочих нагрузок в облаке и изучаете функции безопасности, предоставляемые AWS.

Еще один ключевой элемент вашей стратегии – проектирование модели общей ответственности для вашей экосистемы. Помимо отношений с AWS на макроуровне рекомендуется изучить внутриорганизационные компоненты концепции общей ответственности и компоненты, за которые отвечают ваши партнеры. Модель общей ответственности компании можно подразделить на три важных компонента: структура контроля; модель RACI (исполнение, ответственность, консультирование, информирование); реестр рисков. Система контроля характеризует ожидаемое функционирование разных аспектов безопасности компании и определяет, какие механизмы контроля будут внедрены для управления рисками. Модель RACI можно использовать для идентификации и назначения специалиста ответственным за те или иные механизмы контроля в этой системе. Наконец, необходимо фиксировать в реестре рисков механизмы контроля, владельцев которых должным образом определить не удалось. Определите приоритетность выявленных остаточных рисков, интегрировав меры снижения этих рисков в новые направления деятельности и инициативы по их устранению.

Сопоставляя разные компоненты модели общей ответственности вы, вполне вероятно, обнаружите новые возможности автоматизации операций и оптимизации рабочих процессов ключевых агентов систем безопасности, соответствия требованиям и управления рисками. На рисунке 2 показан пример расширенной модели общей ответственности.

Рис. 2. Пример модели общей ответственности

Несколько важных моментов

- **Разработайте** специализированную стратегию, соответствующую подходу вашей организации к обеспечению безопасности в облаке.
- **Поставьте** автоматизацию во главу угла любой своей стратегии.
- **Четко** сформулируйте свой подход к облаку в первую очередь.
- **Поощряйте** гибкость, определяя диапазоны допустимых значений.
- **Воспринимайте** работу со стратегией как небольшое упражнение, определяющее подход вашей организации к информационной безопасности в облаке.
- **Работайте** быстрыми, небольшими циклами и обязательно зафиксируйте свою стратегию. Ваша цель – создать набор руководящих принципов, с учетом которых ваша организация будет двигаться вперед. Стратегия сама по себе не является вашей конечной целью. Действуйте быстро и будьте готовы адаптироваться и развиваться.
- **Определите** стратегические принципы, которые позволят внедрить нужную корпоративную культуру в сфере безопасности и на которых будут основываться принимаемые вами решения, а не стратегию, подразумевающую конкретные решения.

Итак, в путь! Составляем программу

Сформулировав стратегию, необходимо реализовать ее на практике и инициировать процесс, который позволит преобразовать вашу организацию безопасности и обеспечит безопасный переход к облаку. Несмотря на широкое разнообразие вариантов и функций, затягивать с выбором метода реализации не стоит. Проектирование и внедрение разнообразных функциональных возможностей в комплексе – это отличная возможность быстро войти в курс дела и научиться выполнять циклы проектирования в соответствии с вашими требованиями. Целесообразно как можно раньше извлечь уроки из реальной реализации, а затем адаптировать систему, внося изменения по мере поступления новой информации.

Рисунок 3. Сценарии безопасности AWS CAF

Существенную помощь во внедрении окажут сценарии безопасности CAF (см. рис. 3). Сценарии безопасности – это набор пользовательских историй (примеры использования и примеры нарушений), которые можно использовать во время спринтов. В каждом из этих сценариев – несколько циклов, позволяющих удовлетворить все более сложные требования и создать несколько уровней обеспечения отказоустойчивости. Несмотря на то что мы рекомендуем использовать гибкие системы, эти сценарии можно применять для выделения общих направлений работы, определения приоритетности и структурирования задач при работе с любой другой платформой. Предлагаемая структура состоит из следующих 10 сценариев безопасности (рис. 4), которые помогут выполнить внедрение.

Рис. 4. 10 сценариев безопасности AWS

Базовая пятерка

Следующие пять сценариев посвящены базовым механизмам контроля и функциям, которые необходимо учитывать на ранних этапах реализации, поскольку они играют важную роль в запуске всего проекта.

- **IAM**: система управления идентификацией и доступом AWS Identity and Access Management (IAM) – это краеугольный камень вашего развертывания AWS. Распределять и координировать ресурсы можно только после того, как в облаке будет создан аккаунт и ему будут предоставлены соответствующие привилегии. Как правило, автоматизируются следующие задачи: сопоставление, предоставление и аудит прав, управление конфиденциальными материалами, принудительное разделение обязанностей и доступ по принципу минимальных привилегий, управление привилегиями «на лету» и уменьшение использования долгосрочных учетных данных.
- **Ведение журналов и мониторинг**: сервисы AWS предоставляют большой объем данных журналов, которые можно использовать для мониторинга взаимодействия с платформой. Этот сценарий позволяет оценить эффективность сервисов AWS с учетом выбранных параметров конфигурации и способности использовать журналы ОС и приложений для создания общей эталонной структуры. Как правило, автоматизируются следующие задачи: агрегация журналов, обработка пороговых значений, сигналов и оповещений, обогащение данных, работа с поисковой платформой, визуализация, доступ заинтересованных лиц, рабочие процессы и обработка заявок с целью запуска процедуры реагирования замкнутого цикла в организации.

- **Безопасность инфраструктуры**: если вы рассматриваете инфраструктуру как код, инфраструктура безопасности становится рабочей нагрузкой первого уровня, которую также необходимо развертывать как код. Реализуя такой подход, вы сможете программным образом настраивать сервисы AWS и развертывать инфраструктуру безопасности, компоненты которой предоставляются партнерами AWS Marketplace или разработаны вами самостоятельно. Как правило, автоматизируются следующие задачи: создание пользовательских шаблонов для настройки сервисов AWS в соответствии с вашими требованиями, реализация шаблонов архитектуры безопасности и сценариев использования механизмов безопасности в качестве кода, создание пользовательских решений безопасности на базе сервисов AWS, реализация стратегий управления изменениями (синие/зеленые развертывания), уменьшение поверхности атаки и проверка эффективности развертывания.

- **Защита данных**: обеспечение безопасности важных данных – чрезвычайно важный аспект создания и эксплуатации информационных систем, и AWS предоставляет сервисы и функции для надежной защиты данных на протяжении всего жизненного цикла. Как правило, автоматизируются следующие задачи: принятие решений о размещении рабочей нагрузки, реализация схемы тегов, создание механизмов защиты переносимых данных с использование VPN и подключений TLS/SSL (включая диспетчер AWS Certificate Manager), создание механизмов защиты хранимых данных путем шифрования на соответствующих уровнях инфраструктуры, внедрение и интеграция сервиса AWS Key Management Service (AWS KMS), развертывание AWS CloudHSM, создание схем токенизации, внедрение и эксплуатация партнерских решений с AWS Marketplace.

- **Отклик на инциденты**: автоматизация некоторых аспектов управления инцидентами повышает надежность, ускоряет отклик и позволяет создать среду, которую проще оценить в ходе последующего анализа. Как правило, автоматизируются следующие задачи: использование «механизмов отклика» AWS Lambda, которые реагируют на конкретные изменения среды, координация событий автоматического масштабирования, изоляция подозрительных системных компонентов, развертывание «на лету» средств для проведения расследования, создание рабочих процессов и заявок для завершения инцидента и извлечения уроков из процедуры реагирования замкнутого цикла.

Дополнение к основным сценариям

Эти пять сценариев отражают факторы, которые обеспечат стабильно высокие показатели вашей операционной деятельности благодаря доступности, автоматизации и аудиту. Необходимо взвешенно интегрировать эти сценарии в каждый из спринтов. Если вы хотите рассмотреть какой-то сценарий более тщательно, имеет смысл выделить его в качестве самостоятельного сценария.

- **Отказоустойчивость**: высокая доступность, непрерывность операций, надежность и отказоустойчивость, а также удобство аварийного восстановления – вот причины, по которым все чаще отдают предпочтение облачным развертываниям с использованием AWS. Как правило, автоматизируются следующие задачи: развертывание в нескольких зонах доступности и в нескольких регионах, изменение существующей поверхности атаки, масштабирование и перераспределение ресурсов с целью поглощения атак, защита ресурсов под угрозой и умышленное инициирование сбоя ресурсов с целью проверки непрерывности работы системы.

- **Проверка соответствия**: внедрение комплексных механизмов обеспечения соответствия в вашу программу безопасности не позволит свести меры по обеспечению соответствия требованиям к простому проставлению галочек или превратить их в декоративную задачу, которая решается после развертывания. Этот сценарий предоставляет платформу, которая консолидирует и рационализирует артефакты соответствия требованиям, созданные при реализации других сценариев. Как правило, автоматизируются следующие задачи: создание модульных тестов безопасности, сопоставленных требованиям соответствия, разработка сервисов и рабочих нагрузок, обеспечивающих поддержку сбора доказательств соответствия требованиям, создание каналов визуализации соответствия требованиям (с использованием функций для работы с доказательствами) и распространения соответствующих уведомлений, непрерывный мониторинг, создание групп специалистов по разработке, обеспечению безопасности и эксплуатации с развитыми навыками использования инструментов соответствия требованиям.

- **Безопасность непрерывной интеграции и непрерывного развертывания (DevSecOps)**: уверенность в своей цепочке поставок программного обеспечения благодаря использованию надежных и проверенных наборов инструментов для непрерывной интеграции и непрерывного развертывания – надежный способ повышения зрелости практических мер безопасности при переходе в облако. Как правило, автоматизируются следующие задачи: укрепление набора инструментов и внесение исправлений, доступ к набору инструментов по принципу минимальных привилегий, мониторинг производственного процесса и ведение журналов, визуализация интеграции и развертывания механизмов безопасности, проверка целостности кода.

- **Анализ конфигурации и уязвимостей**: масштабируемость, гибкость и возможности автоматизации, которые обеспечивает AWS, являются существенными преимуществами для анализа конфигурации и уязвимостей. Как правило, автоматизируются следующие задачи: реализация AWS Config и создание пользовательских правил AWS Config, использование Amazon CloudWatch Events и AWS Lambda для реагирования на обнаруженные изменения, внедрение Amazon Inspector, выбор и развертывание решений непрерывного мониторинга на AWS Marketplace, развертывание инициируемых проверок и внедрение инструментов оценки в наборы инструментов непрерывной интеграции и развертывания.

- **Большие данные о безопасности и прогнозная аналитика**: сервисы и решения для работы с большими данными обеспечивают те же преимущества в сфере обеспечения безопасности, что и в любых других отраслях деятельности. Использование больших данных открывает своевременный доступ ко всеобъемлющим ценным сведениям, повышает гибкость вашей деятельности и способность реализовывать меры безопасности по нарастающей. Как правило, автоматизируются следующие задачи: создание утечек данных о безопасности, разработка аналитических каналов, создание визуализаций, используемых в принятии решений в сфере безопасности и внедрение механизмов обратной связи для автономного отклика.

После определения этой структуры можно переходить к созданию плана реализации. Со временем ваши возможности меняются, непрерывно выявляются возможности для совершенствования. Напоминаем, что в рамках гибкой методики категории «темы» или «возможности» (см. выше) можно рассматривать как сценарии, которые содержат несколько пользовательских историй, в том числе примеры использования и примеры нарушений. После нескольких спринтов система станет более зрелой и сохранит гибкость, то есть возможность адаптироваться к темпу и потребностям вашего бизнеса.

Примеры последовательностей спринтов

Пробный проект можно разделить на шесть двухнедельных спринтов (группа сценариев будет реализована за календарный квартал, 12 недель) и короткий подготовительный период следующим образом. Используемый подход буде зависеть от доступности ресурсов, приоритетов, желаемого уровня зрелости каждой функции при переходу к минимально допустимому уровню возможности в производственной среде (MVP).

- **Спринт 0**. Составление карты безопасности: сопоставление соответствия требованиям, сопоставление политик, анализ первоначальной модели угроз, составление реестра рисков; создание журнала невыполненных работ по примерам использования и примерам нарушений за прошлые периоды, планирование сценариев безопасности
- **Спринт 1**. Управление идентификацией и доступом, ведение журналов и мониторинг
- **Спринт 2**. Управление идентификацией и доступом, ведение журналов и мониторинг, защита инфраструктуры
- **Спринт 3**. Управление идентификацией и доступом, ведение журналов и мониторинг, защита инфраструктуры
- **Спринт 4**. Управление идентификацией и доступом, ведение журналов и мониторинг, защита инфраструктуры, защита данных
- **Спринт 5**. Защита данных, автоматизация операций в сфере безопасности, планирование отклика на инциденты и использования инструментов, отказоустойчивость
- **Спринт 6**. Автоматизация операций в сфере безопасности, отклик на инциденты, отказоустойчивость

Ключевой элемент проверки соответствия требованиям – включение элементов проверки в каждый спринт в составе модульных тестов безопасности и соответствия требованиям с последующим выходом на уровень производственных процессов. Если требуется функция явной проверки соответствия требованиям, можно создать спринты, в ходе которых будут проверяться конкретные пользовательские истории. Со временем благодаря цикличности можно наладить процесс непрерывной проверки и автоматического внесения исправлений по любым отклонениям.

В общем и целом такой подход имеет целью точно определить базовый показатель (или минимально допустимый уровень возможности в производственной среде), который затем будет сопоставляться первому спринту в каждой области. На начальных этапах конечная цель, возможно, будет определена не столь четко, однако должен быть создан однозначный пошаговый план первоначальных спринтов. Время, опыт и постоянные повторения позволят получить оптимальный результат, который требуется именно вашей организации. В реальности конечное состояние может непрерывно меняться, но в конечном счете описанная процедура приведет к непрерывному и более быстрому совершенствованию. Такой подход может оказаться более эффективным и экономичным, чем так называемая стратегия «большого взрыва» с внушительными сроками и вложениями.

Если копнуть немного глубже, очевидным становится следующее: первый спринт, включающий управление идентификацией и доступом, может включать определение структуры аккаунтов и реализацию базового набора рекомендаций. Во втором спринте можно реализовать концепцию федерации. В третьем спринте можно расширить управление аккаунтами до управления большим числом аккаунтов и т. д. Пользовательские истории IAM, которые могут охватывать один или несколько следующих исходных спринтов, могут включать следующее:

«Я – администратор доступа, и я хочу создать исходный круг пользователей для управления привилегированным доступом и отношениями доверия с поставщиком федеративных удостоверений».

«Я – администратор доступа, и я хочу сопоставить пользователей в существующем корпоративном каталоге функциональным ролям (или наборам прав доступа) на платформе AWS».

«Я – администратор доступа, и я хочу реализовать MFA (multi-factor authentication) для всех операций, выполняемых интерактивными пользователями с консолью AWS».

Пользовательские истории ведения журналов и мониторинга могут охватывать один или несколько следующих исходных спринтов:

«Я – аналитик мер безопасности, я хочу получать зафиксированные в журнале данные уровня платформы для всех регионов и аккаунтов AWS».

«Я – аналитик мер безопасности, я хочу, чтобы все журналы уровня платформы для всех регионов и аккаунтов AWS доставлялись в одно общее расположение».

«Я – аналитик мер безопасности, и я хочу получать уведомления о любых операциях, в ходе которых политики IAM применяются в отношении пользователей, групп или ролей».

Функции можно создавать параллельно или последовательно, включая пользовательские истории функций безопасности в общий журнал невыполненных работ по продукту. Кроме того, пользовательские истории можно выделить в сферу ответственности группы специалистов по разработке и эксплуатации с акцентом на безопасность. Эти решения нужно периодически пересматривать, адаптируя метод реализации к меняющимся со временем нуждам организации.

Несколько важных моментов

- **Анализируйте** существующую систему контроля, чтобы определить, как с помощью сервисов AWS обеспечить соблюдение требуемых стандартов безопасности.
- **Определите** пользователей, а затем составьте подробный план их взаимодействия с сервисами AWS.
- **Определите**, что нужно сделать в первом спринте и какова первоначальная общая цель на более долгосрочный период.
- **Обозначьте** минимально допустимые для нормального функционирования системы базовые показатели безопасности и непрерывно работайте над повышением планки для рабочих нагрузок и данных, безопасность которых вы обеспечиваете.

Итак, в путь! Разработка надежных мер безопасности

В среде, где инфраструктура является кодом, безопасность также необходимо расценивать в качестве кода. Компонент«Меры безопасности» предоставляет все необходимое для доведения концепции «безопасность как код» до сведения коллектива и реализации этой концепции на практике.

- Использование облака для защиты облака.
- В инфраструктуре безопасности необходимо обеспечить поддержку облака.
- Воспользуйтесь API, чтобы реализовать функции безопасности как сервисы.
- Автоматизируйте все процессы, чтобы обеспечить возможность масштабирования мер безопасности и обеспечения соответствия требованиям.

Для успешной реализации этой модели управления на практике бизнес-подразделения часто формируют группы специалистов по разработке и эксплуатации для создания и развертывания инфраструктурного ПО и бизнес-приложений. Базовые компоненты этой модели управления можно расширить, интегрировав безопасность в корпоративную культуру (или практику) разработки и эксплуатации – иногда это образование называют DevSecOps. Рабочую группу необходимо строить на основе следующих принципов:

- Группа должна принять культуру и модели поведения DevOps.
- Разработчики открыто участвуют в создании кода для автоматизации мер безопасности.операция
- Рабочая группа по безопасности имеет право участвовать в тестировании и автоматизации кода приложений.
- Группа гордится тем, как быстро и часто развертываются новые компоненты. Более частое развертывание с небольшими изменениями снижает операционные риски и позволяет быстрее реализовать стратегию безопасности.

Интегрированная группа специалистов по разработке, безопасности и эксплуатации имеет три основные общие миссии.

- Укрепление набора инструментов непрерывной интеграции и непрерывного развертывания.
- Обеспечение возможности и поощрение разработки отказоустойчивого программного обеспечения с использованием данного набора инструментов.
- Развертывание всех компонентов инфраструктуры безопасности и программного обеспечения с использованием этого набора инструментов.

Решение вопроса о том, помогут ли изменения (если применимо) в существующей практике безопасности спланировать стратегию плавного освоения AWS.

Заключение

Приступая к освоению AWS, вы наверняка захотите обновить свою систему безопасности с учетом новых компонентов среды – компонентов AWS. В техническом описании «Перспектива безопасности» даются пошаговые инструкции и рекомендации по реализации всех преимуществ AWS для безопасности вашей системы. На веб-сайте AWS вы найдете гораздо больше информации о безопасности: там детально описаны функции безопасности и даны подробные инструкции для стандартных реализаций. Там же доступен полный список материалов по безопасности[4], которые должны изучить разные специалисты вашей группы безопасности во время подготовки к освоению AWS.

Приложение A. Отслеживание прогресса для перспективы безопасности AWS CAF

Для оценки хода выполнения и зрелости реализации перспективы безопасности AWS CAF можно использовать ключевые факторы безопасности и модель выполнения на основе сценариев безопасности, описанные в этом приложении. Эти факторы и модель выполнения можно использовать и для планирования проектов, оценки отказоустойчивости реализаций или просто как инструмент обсуждения дальнейших планов.

Ключевые факторы безопасности

Ключевые факторы безопасности – это вехи, которые позволяют не сбиться с пути. Мы используем модель оценки из трех значений: не выполнено, выполняется и выполнено.

- Стратегия облачной безопасности [не выполнено, выполняется и выполнено]
- План взаимодействия с заинтересованными лицами [не выполнено, выполняется и выполнено]
- Карта безопасности [не выполнено, выполняется и выполнено]
- Документирование модели общей ответственности [не выполнено, выполняется и выполнено]
- Меры безопасности: сценарии и перечни задач [не выполнено, выполняется и выполнено]
- План сценариев безопасности [не выполнено, выполняется и выполнено]
- Моделирование отклика на инциденты безопасности [не выполнено, выполняется и выполнено]

Модель выполнения сценариев безопасности

Модель выполнения на основе сценариев безопасности позволяет оценить реализацию 10 сценариев безопасности, описанных в этом документе. Для оценки отказоустойчивости используется шкала от 0 (нуля) до 3. В качестве примера рассмотрим сценарии «Управление идентификацией и доступом» и «Ведение журналов и мониторинг», чтобы вы увидели шкалу в действии.

Пять базовых сценариев безопасности

0 – не выполнено

1 – выполнено в архитектуре и планах

2 – выполнено на минимально допустимом уровне

3 – выполнено в производственной среде, готово к выполнению в масштабах организации

Сценарий безопасности	0	1	2	3
Управление идентификацией и доступом	Пример: нет связи между локальными удостоверениями и удостоверениями AWS.	Пример: определен подход к управлению удостоверениями на протяжении жизненного цикла рабочих ресурсов; архитектура IAM документирована; рабочие функции сопоставлены потребностям политики IAM.	Пример: система IAM реализована в соответствии с определением в архитектуре; реализованы политики IAM, соответствующие определенным рабочим функциям; реализация IAM проверена.	Пример: автоматизация рабочих процессов жизненного цикла IAM;
ведение журналов и мониторинг.	Пример: не используются предоставленные AWS решения для ведения журналов и мониторинга.	Пример: определен подход к созданию журналов, мониторингу и интеграции в процессы управления событиями безопасности.	Пример: ведение журнала на уровне платформы и на уровне сервиса включено и осуществляется централизованно.	Пример: события, имеющие последствия для безопасности, глубоко интегрированы в рабочий процесс обеспечения безопасности, процессы и системы управления инцидентами.
Безопасность инфраструктуры				
Защита данных				
Управление инцидентами				

Дополнение к 5 основным сценариям

0 – не выполнено

1 – выполнено в архитектуре и планах

2 – выполнено на минимально допустимом уровне

3 – выполнено в производственной среде, готово к выполнению в масштабах организации

Сценарий безопасности	**0**	**1**	**2**	**3**
Отказоустойчивость				
DevSecOps				
Проверка соответствия требованиям				
Управление конфигурацией и уязвимостями				
Большие данные о безопасности				

Классификация и определения CAF

План освоения облака (CAF) – это платформа, созданная AWS, чтобы объединить все рекомендации и инструкции из прошлых проектов заказчиков. *Перспектива* AWS CAF – это направление, актуальное для реализации облачных ИТ-систем в организациях. Например, перспектива безопасности предоставляет инструкции и процедуры для оценки и совершенствования существующих механизмов контроля безопасности при переходе к среде AWS.

Каждая перспектива CAF состоит из определенных компонентов и действий. *Компонент* – это область более низкого уровня в составе перспективы, которая представляет определенный аспект, требующий внимания. В этом техническом описании рассматриваются компоненты перспективы «Безопасность». *Действие* предоставляет более предписывающие инструкции по созданию практических планов, с помощью которых организация может перейти к облаку и эксплуатировать облачные решения на постоянной основе.

Так, *директивный* компонент – один из компонентов перспективы «Безопасность», а адаптация модели общей ответственности AWS для вашей экосистемы – действие в составе этого компонента.

План освоения облака (CAF) и методику освоения облака (CAM) можно использовать в качестве инструкции по переходу к облаку AWS.

Примечания

[1] https://do.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

[2] https://aws.amazon.com/compliance/

[3] https://aws.amazon.com/compliance/shared-responsibility-model/

[4] https://aws.amazon.com/security/security-resources/