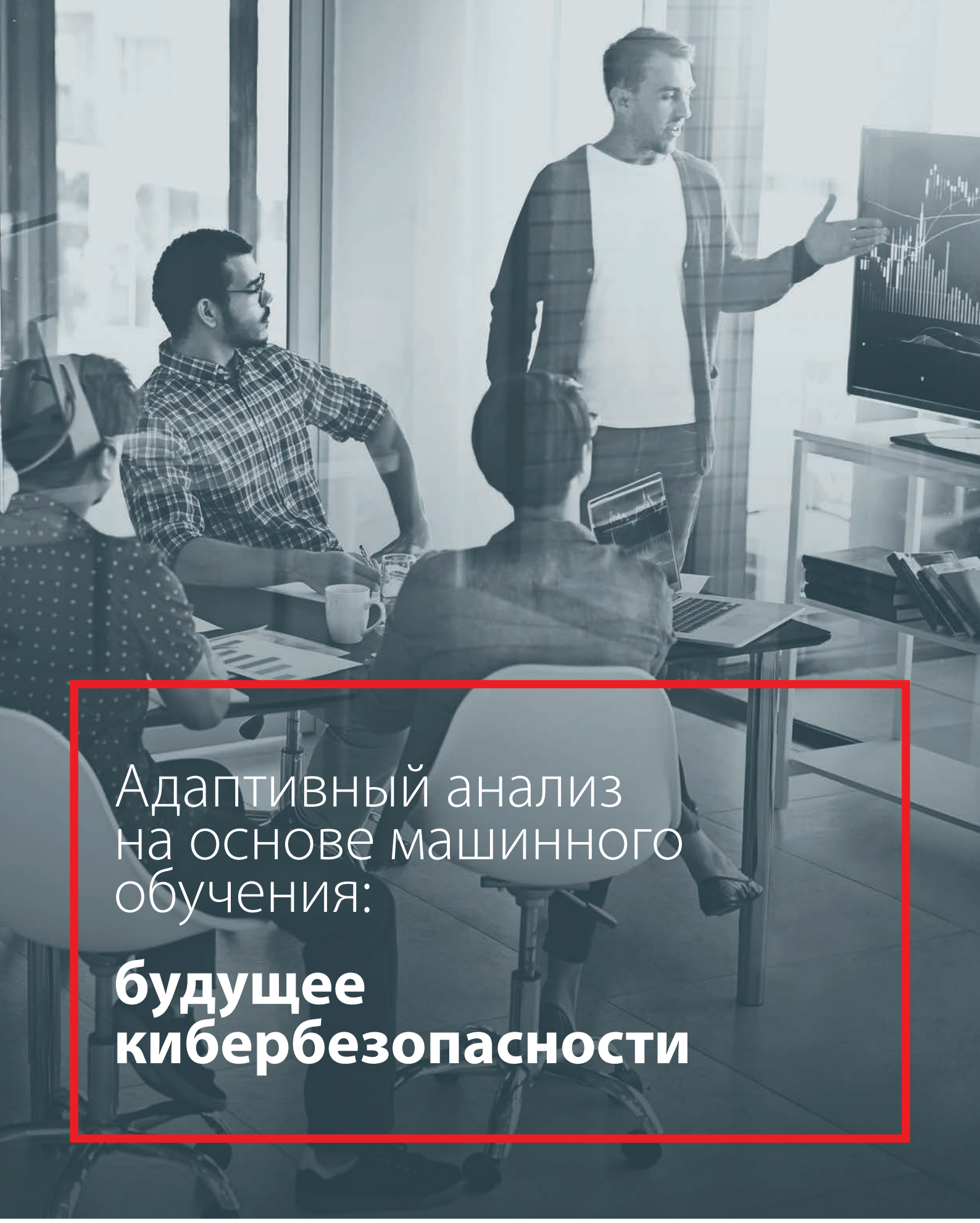


Адаптивный анализ на основе машинного обучения:

будущее кибербезопасности

Официальный документ. Январь 2018 г.

ORACLE

Специалисты центров мониторинга безопасности SOC обновляют пассивные статические стратегии с помощью современных, проактивных сценариев безопасности — адаптивных, непрерывных, интеллектуальных и действующих в реальном времени.

Введение

Большинство компаний переходят на облачные технологии для использования цифровых возможностей для развития бизнеса. Всем нравится удобство облачных сервисов, которые можно быстро и просто резервировать, развертывать и использовать. Однако угрозы безопасности не исчезают с переходом в облако, а масштаб служб в облачной и локальной средах требует нового подхода к киберзащите. Современные компании отказываются от ручного управления стратегиями безопасности в пользу интеллектуальных центров мониторинга безопасности (Security Operations Center). SOC способны прогнозировать, обнаруживать, предотвращать угрозы и реагировать на них автоматически, а также обнаруживать взаимосвязи данных и анализировать журналы событий, чтобы извлекать ценную оперативную информацию.

Ларри Элисон, председатель совета директоров и глава Oracle, в своем докладе на конференции Oracle OpenWorld 2017, объяснил: «Путь к безопасности наших данных и предотвращению их утечки лежит через все большую автоматизацию. И нам нужна система защиты киберпространства, способная автоматически обнаруживать уязвимости и атаки. Устранять уязвимости до атаки. И затем, если атака действительно произойдет, обнаружить и пресечь ее». Он также сказал следующее: «...нам нужны новые системы. Речь не о наших людях против их компьютеров. Такую войну мы проиграем. Это должны быть наши компьютеры против их компьютеров. И не сомневайтесь: это — война».

Как специалисты SOC компенсируют потерю контроля над пользователями, устройствами и приложениями? Насколько они доверяют внешним пользователям (и сотрудникам, работающим вне офиса), которым требуется доступ в их системы? По результатам исследования потерь, связанных с атаками на данные, проведенного институтом Ponemon в 2016 г. (2016 Ponemon Cost of Data Breach Study), в среднем уязвимость обходится крупным компаниям в 4 млн. долл. США, а на обнаружение уходит 99 дней. Отчасти эта статистика является результатом сигналов тревоги множества поставщиков, продуктов, консолей и средств обеспечения безопасности. Слишком много шума, но недостаточно качественной информации для реагирования.

Для защиты корпоративных ИТ-ресурсов и отражения все более современных атак дальновидные организации переходят на адаптивные, непрерывные и интеллектуальные технологии кибербезопасности, действующие в реальном времени. В их основе лежат алгоритмы искусственного интеллекта (ИИ) и машинного обучения (МО) для управления конфигурациями, отслеживания доступа к определенным ресурсам и шифрования особо важных данных для защиты ИТ-ресурсов.

Отражение сложных, автоматизированных угроз

Отрасль информационной безопасности меняется быстрее, чем когда-либо. Периметр сети четко не определен и расширяется по мере роста количества устройств, сервисов и пользователей, которым разрешен доступ к приложениям и данным. Стали обычными автоматизированные угрозы — не от злоумышленника, пытающегося скомпрометировать вашу ИТ-среду с консоли, а от автоматической программы, выполняющей специальные скрипты в попытке проникнуть в ваши системы. Традиционные средства управления безопасностью установлены, но число сообщений о нарушениях от них неконтролируемо растет. И киберпреступники часто остаются незамеченными в этом шуме. Центры мониторинга информационной безопасности получают миллионы тревожных сигналов, поэтому для их сортировки, автоматической обработки и реагирования на них требуются новые подходы.

Кроме того, большинство традиционных средств обеспечения безопасности не были предназначены для облачных сред и решения соответствующих задач — проверки политик безопасности и создания прозрачной инфраструктуры безопасности. Решения о том, кому и к каким ресурсам предоставлять доступ, должны приниматься моментально в зависимости от обстоятельств или контекста каждого запроса. Область доверия уже невозможно определить точно. Специалисты по безопасности должны идентифицировать каждого пользователя или приложение, рассмотреть ресурсы, доступ к которым запрашивается, и учесть степень конфиденциальности соответствующих данных или контента.

Правильное решение о предоставлении доступа к ИТ-ресурсам редко бывает очевидным. Службы безопасности должны постоянно оценивать риски, чтобы отличить злоумышленника. Средства машинного обучения и облачной аналитики способны автоматически обнаруживать аномалии в поведении пользователей, а также перехватывать мошеннические приложения, которые обходят традиционные системы безопасности на периметре. Новые инструменты безопасности на основе правил сканируют данные, которые были пропущены такими системами. Этот вид автоматизации очень важен для SOC, так как обеспечивает быстрое обнаружение и реагирование.

Чтобы динамически определять уровень доверия и рисков, службы безопасности должны быть в состоянии разобраться в тревожных сигналах от самых разных систем, приложений и наборов данных. К ним относятся журналы систем и приложений, данные мониторинга сеансов пользователей, а также данные о том, как осуществляется доступ к важным ресурсам и как меняются конфигурации безопасности. Все системы и устройства следует считать потенциально скомпрометированными в каждый момент времени, и поведение всех пользователей должно постоянно оцениваться для выявления мошеннических, недобросовестных или других вредных действий — случайных или умышленных.

Комплексный портфель безопасности должен быть основан на «модели нулевого доверия». Это означает, что никакого доверия к пользователю, устройству или приложению не подразумевается и что любая форма доверия должна быть определена и реализована с помощью политик и модели прав. Идентифицированным пользователям следует предоставлять ровно столько прав и полномочий, сколько необходимо для выполнения определенных действий. Чтобы делать это системно, специалистам по безопасности требуется знание контекста, оперативные данные и более полная оценка «серых зон», в которых проходит значительная доля современного сетевого трафика. Один и тот же строгий подход должен применяться ко всем средам — облачным, локальным и размещенным.

Межсетевые экраны, системы предотвращения вторжений и другие виды превентивных технологий безопасности являются важной частью защиты информационных активов вашей компании, но не могут обезопасить от новых угроз из облачной и мобильной сред.

Быстрое обнаружение и устранение

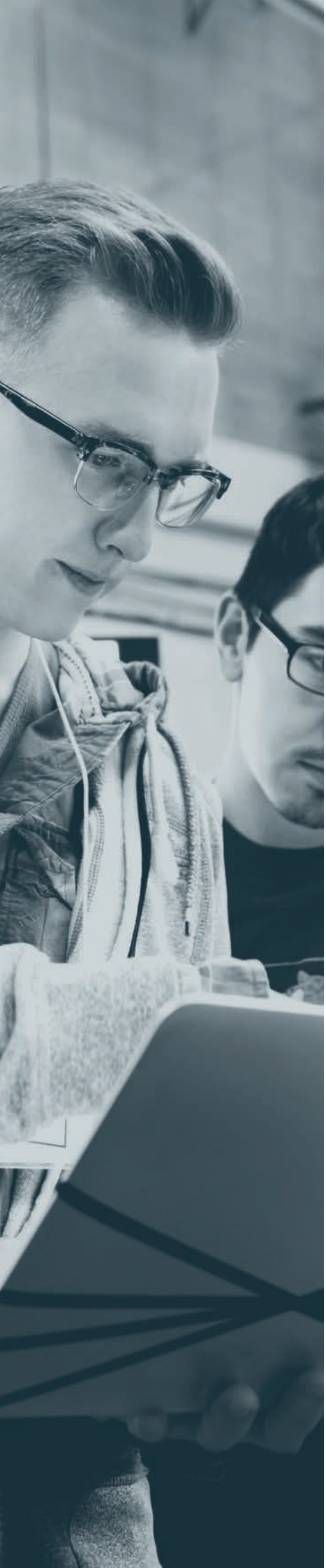
Эффективность системы безопасности сводится к двум основным метрикам: как быстро вы можете обнаружить нарушение и как быстро вы можете отреагировать на известную атаку. Эти две важные метрики известны под названиями «среднее время обнаружения» (mean time to detect, MTTD) и «среднее время реагирования» (mean time to respond, MTTR).

Традиционные средства обеспечения безопасности используют базы данных от надежных партнеров с информацией об известных угрозах. Сегодня этого недостаточно, так как периметр современной сети предприятия четко не определен и первый признак новой и неизвестной угрозы может быть зарегистрирован в журнале приложения или средстве мониторинга сеанса пользователя. Эффективно используя искусственный интеллект и машинное обучение, новые решения обращаются к таким источникам информации для управления системами, как журнальные файлы, бизнес-транзакции, конфигурации приложений, назначения ролей и прав и другие источники, неизвестные традиционным средствам обеспечения безопасности. Технологии искусственного интеллекта и машинного обучения помогут прослеживать связь событий и применять эвристику для выявления шаблонов, тенденций и аномалий в данных, включая обнаружение новых тревожных сигналов, добавление контекста к ним, быстрое реагирование и устранение инцидентов. Автоматическое решение для обеспечения облачной безопасности может постоянно оценивать миллионы шаблонов и выявлять аномалии и подозрительные действия.

Алгоритмы машинного обучения хорошо масштабируются для работы с большими объемами данных, если они развернуты в облаке. Если же выбрано локальное решение, то инфраструктура быстро расширяется и требует все новых ресурсов для нужд обработки и хранения. Алгоритм искусственного интеллекта обрабатывает данные для выявления шаблонов, создания аудиторских отчетов и обнаружения рисков для системы безопасности на основе предопределенных моделей угроз, базовых индикаторов риска, аномальных событий и подозрительных действий пользователей.

Далее в этом документе показано, как технологии искусственного интеллекта (ИИ) и машинного обучения (МО) могут оптимизировать основные операции в центрах эксплуатации сети и мониторинга информационной безопасности.

Аналитика безопасности на основе машинного обучения



Постоянное обнаружение

Современные разнообразные вычислительные среды требуют интеллектуальной инфраструктуры безопасности, способной постоянно отслеживать потенциальные угрозы и реагировать на подозрительное поведение. Цель — избавиться от ложных срабатываний, максимально исключить малозначимые детали из миллионов тревожных сообщений и автоматизировать такую простую работу, как повышение уровней аутентификации, там, где требуется запрещать доступ неавторизованным пользователям.

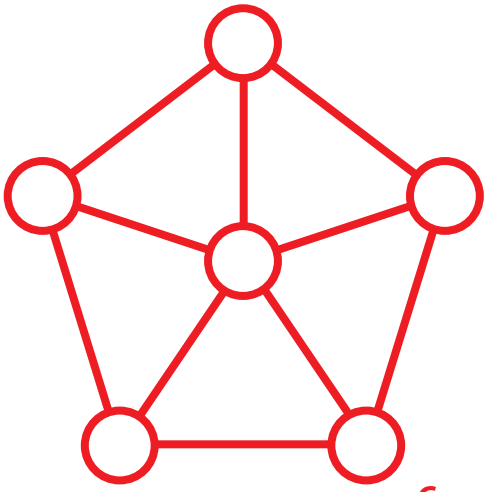
У Oracle есть набор облачных сервисов, который обеспечивает большую прозрачность, эффективный анализ и автоматизацию информационной безопасности. Все эти сервисы работают на платформе Oracle Management Cloud (OMC). Это интегрированный набор служб мониторинга, управления и анализа, использующий технологии машинного обучения и больших данных для работы с самыми разными наборами операционных данных. Например, сервис Oracle Configuration and Compliance Cloud Service позволяет персоналу службы ИТ и службы безопасности оценивать нарушения по степени серьезности и устранять их, используя для этого отраслевые стандарты в дополнение к правилам, заданным пользователем. Сервис Oracle Security Monitoring and Analytics (SMA) Cloud Service позволяет быстро обнаруживать, расследовать и устранять угрозы безопасности и сопоставляет результаты с привилегиями, назначенными на платформе управления идентификацией и доступом (Identity and Access Management, IAM) или Active Directory.

Сервис Oracle Orchestration Cloud Service обеспечивает автоматическое реагирование администраторами по защите данных на инциденты, тревожные сообщения и события, а также включает возможность задавать правила, используя любые языки выполнения сценариев и ПО для настройки конфигураций.

Когда облачные службы безопасности Oracle извещают СУБД об уязвимостях, она оперативно применяет необходимые исправления. Кроме того, она обнаруживает аномальные SQL-запросы путем синтаксического анализа SQL-комманд и устанавливает критерии для «белых» списков по пользователям, группам, базам данных и приложениям. Новые SQL-запросы сопоставляются с такими базовыми критериями для обнаружения потенциальных угроз, их оценки и принятия мер для защиты важных данных. На стороне сервера Oracle Autonomous Database Cloud Service упрощает администрирование баз данных и настройку задач, включая автоматическое обслуживание конфигураций безопасности.

Первая в мире автономная СУБД

Самоуправление
Пользователь задает уровень сервиса, а СУБД его обеспечивает



Самовосстановление
Автоматическая защита от любых сбоев

Самонастройка
Постоянная адаптивная настройка производительности

Самозащита
Защита от внешних и внутренних угроз

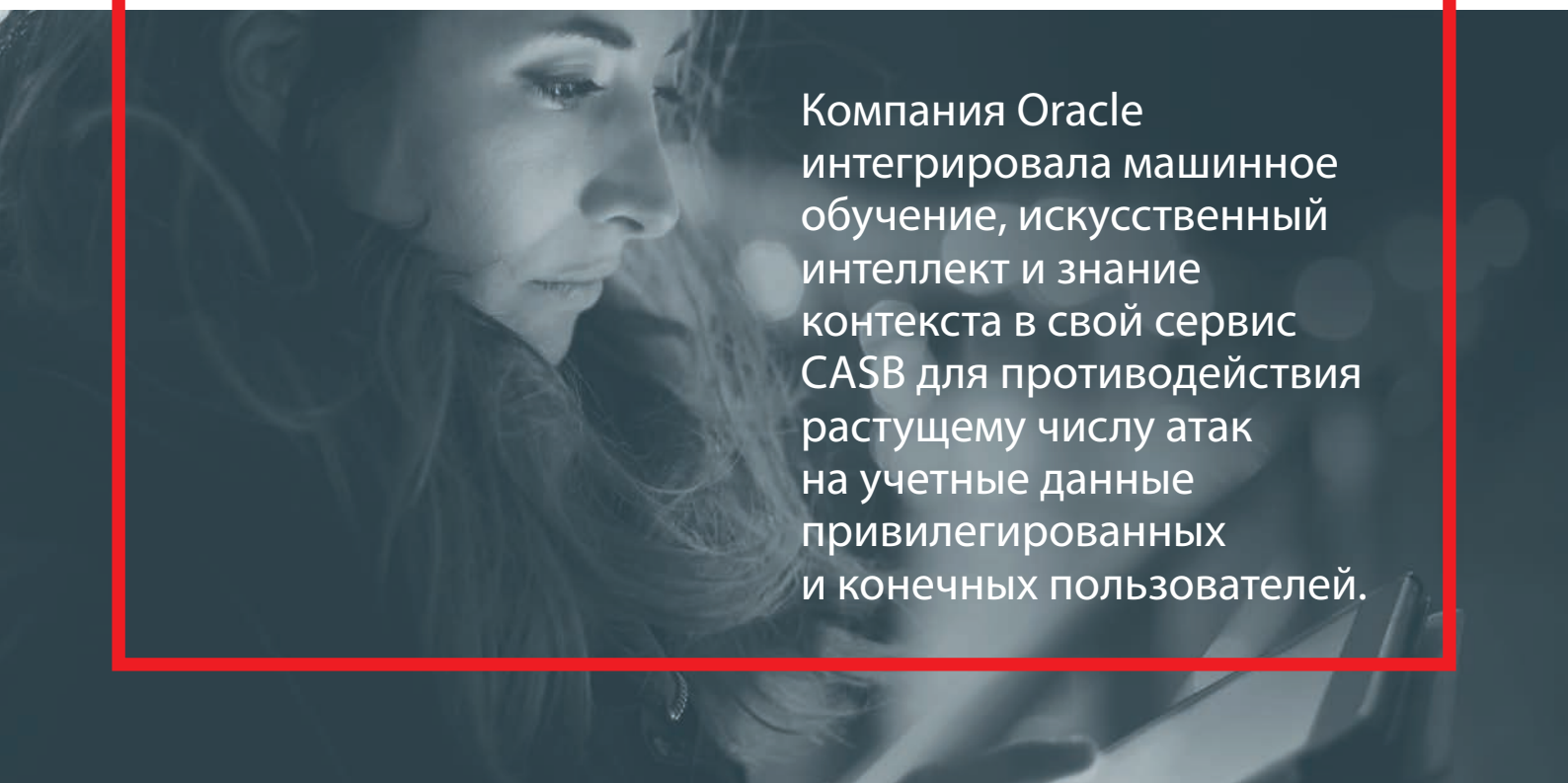
Самомасштабирование
Мгновенное изменение вычислительной мощности и емкости хранилища без простоев

Снижение трудозатрат, расходов и количества ошибок, повышение защиты и надежности

Адаптивное реагирование

Современная система безопасности может адаптироваться к меняющимся условиям благодаря технологии машинного обучения, которая автоматически выявляет и устраняет проблемы без участия человека. Это так называемое адаптивное реагирование. Важность такой автоматизации растет в современных гибридных облачных средах. Например, вы можете практически не знать, как люди используют свои мобильные устройства для загрузки приложений и данных через корпоративную сеть. Многие сотрудники используют Box, Dropbox, Evernote, Office 365 и другие облачные приложения для разных нужд, а также личные учетные записи Gmail для отправки и приема корпоративных данных. Это удобно для пользователей, но без строгих правил служба ИТ может потерять контроль над использованием этих приложений, соответствующими данными и их хранением.

Крупные организации обычно имеют сотни облачных сервисов. Лучшие поставщики облачных услуг эффективно защищают свою инфраструктуру, но клиенты должны сами защищать свои данные в облаке. Утечки данных и атаки возможны, если у компании нет достаточно эффективных систем идентификации и управления доступом. Кроме того, интерфейсы прикладного программирования (API-интерфейсы) и пользовательские интерфейсы имеют IP-адреса, доступные за пределами безопасного периметра организации. Поскольку эти активы не защищены, они могут стать мишенями для атак через Интернет.

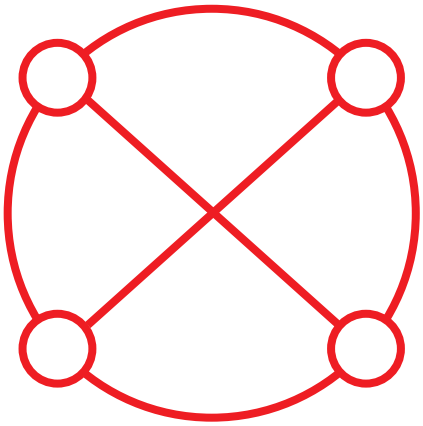


Компания Oracle интегрировала машинное обучение, искусственный интеллект и знание контекста в свой сервис CASB для противодействия растущему числу атак на учетные данные привилегированных и конечных пользователей.

Сервис Cloud Access Security Broker (CASB) поможет в управлении облаком, выступая в качестве посредника между пользователями и поставщиками облачных услуг и консолидируя действия, направленные на соблюдение политик безопасности. Например, сервис Oracle CASB Cloud Service защищает критические данные в облачных службах, обеспечивая прозрачность, обнаружение угроз, нормативно-правовое соответствие и автоматическое реагирование на основе единой платформы. Этот сервис, находящийся между вашей локальной инфраструктурой и инфраструктурой поставщика облачных услуг, действует как контролер, позволяющий распространить внутренние политики безопасности за пределы вашей инфраструктуры. Пользователи могут получить безопасный доступ к облачным сервисам с ПК за межсетевым экраном или с мобильного устройства в кофейне. Ваша служба безопасности теперь получает информацию о теневых ИТ-процессах и может уверенно разрешать использование санкционированных облачных сервисов, включая Amazon Web Services, Google Apps и Salesforce.

Прозрачность облака
Прозрачность всех типов облачных сервисов (включая теневые ИТ-процессы, корпоративные приложения, магазин App Store и клиентские приложения)

Автоматизация соответствия требованиям
Конфигурации на основе лучших практик с клиентскими настройками для уникальных требований ИТ

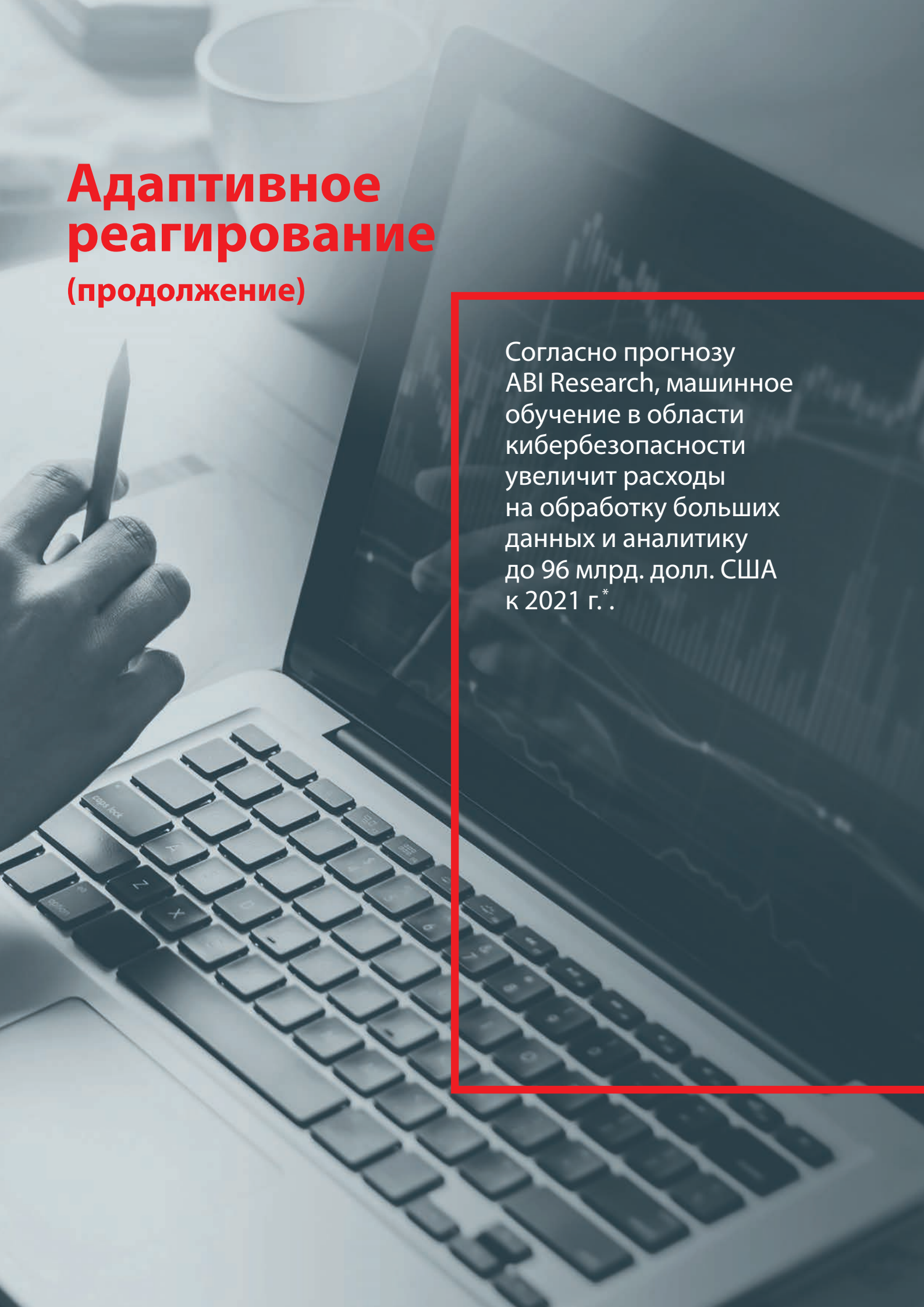


Обнаружение угроз
Обнаружение угроз из всех типов облачных сервисов

Защита данных
Отслеживание доступа к данным, их перемещения, копирования, переименования, изменения, удаления и блокировки

Адаптивное реагирование

(продолжение)



Согласно прогнозу ABI Research, машинное обучение в области кибербезопасности увеличит расходы на обработку больших данных и аналитику до 96 млрд. долл. США к 2021 г.*.

Сервисы CASB используют анализ поведения пользователей и иных сущностей (user entity behavior analytics, UEBA) для определения уникальных критериев поведения для каждого пользователя и облачного сервиса. Они постоянно сравнивают необычные действия с этими ожидаемыми характеристиками для выявления аномального, подозрительного или потенциально рискованного поведения. Обнаружив отклонение, CASB запускает интеллектуальную реакцию. В частности, CASB может взаимодействовать с системой регистрации инцидентов и управления ими для сравнения события с аналогичными случаями и предложения целевого решения с участием сотрудника.

Используя алгоритмы машинного обучения, сервис Oracle CASB определяет типичное поведение для каждого приложения. Определяются базовые критерии типичного поведения пользователя, отклонения от которого можно измерить. Если поведение пользователя выходит за пределы обоснованно ожидаемого, такое поведение может быть отмечено как аномальное. Например, если семья сотрудника проживает на Украине и время от времени сотрудник работает оттуда, такой вход в систему не будет отмечен как индикатор риска. Но, если сотрудник, никогда не посещающий Украину, вдруг входит в систему из этой страны, система может использовать механизм адаптивного контроля доступа в CASB и многофакторную аутентификацию, запустив процедуру двухфакторной идентификации для проверки личности пользователя.

Таким образом, система безопасности становится все более интеллектуальной. Чем больше данных она исследует, чем больше пользователей узнает и чем больше приложений оказываются в поле ее зрения, тем проще выявлять подозрительное или опасное поведение. Например, CASB может отслеживать приложения, обычно используемые пользователями, места, откуда пользователи входят в систему, способ получения доступа к облачным сервисам и время суток, когда пользователи чаще всего бывают в сети. Если сервис CASB подозревает, что учетные данные могли быть украдены, он может потребовать смены пароля или запустить процедуру двухфакторной аутентификации.

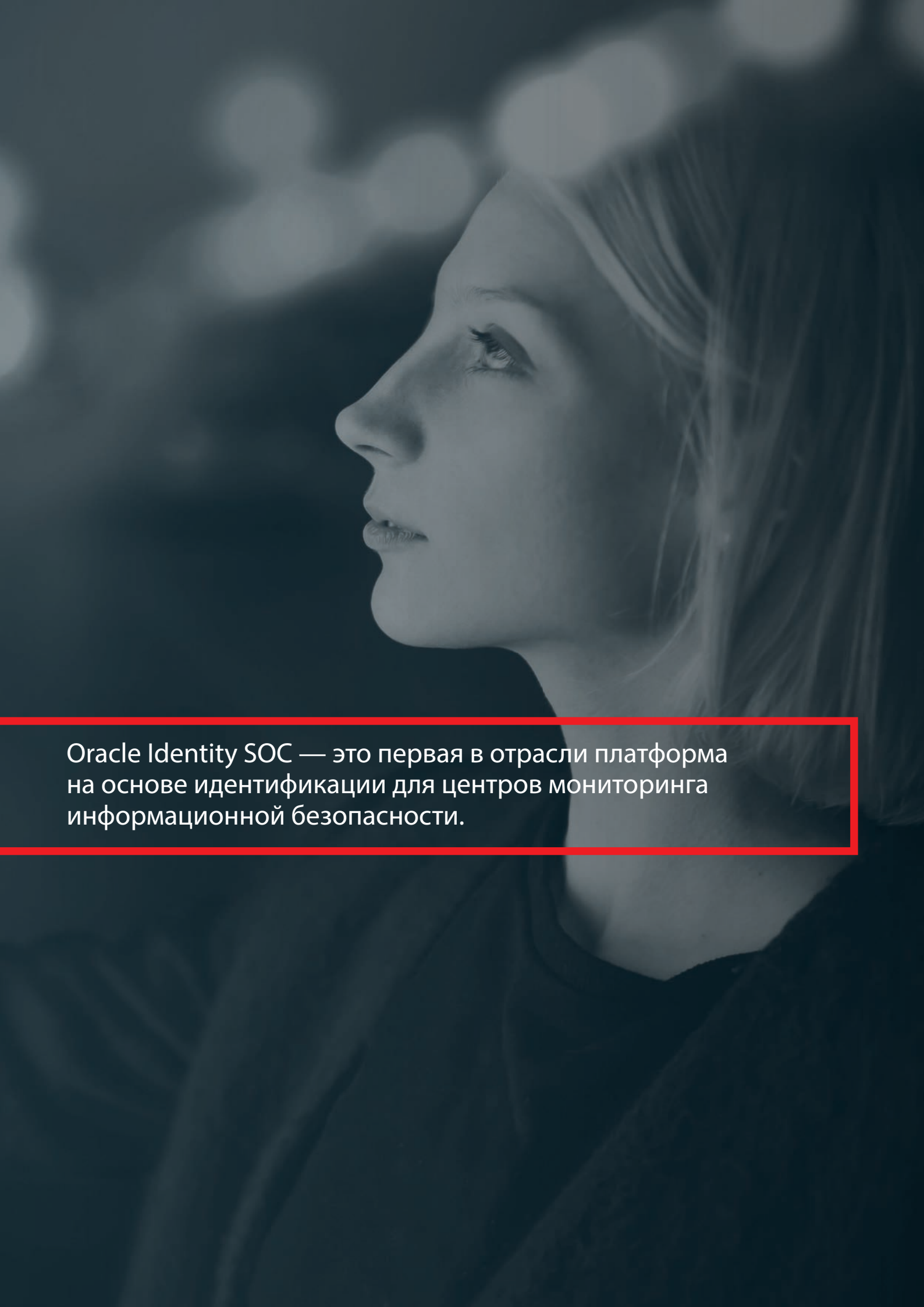
Источник: https://www.abiresearch.com/press/machine-learning-cybersecurity-boost-big-data-inte/.

Анализ рисков на основе идентичности и контекста

Организации, предпочитающие облачную инфраструктуру, реже демонстрируют несоответствие отраслевым и государственным нормам, рекомендациям и стандартам. Однако ввиду новых задач и рисков, пришедших с облачной моделью, сейчас как никогда важен проактивный подход к информационной безопасности. Необходимо создать процессы управления для оценки степени нормативно-правового соответствия и затрат на устранение возможных несоответствий. SOC на основе идентификации использует машинное обучение для лучшего противодействия мошенничеству через облачные и локальные приложения. Для этого анализируется каждая попытка входа вместе с данными о местоположении, устройстве и времени события. Эти интеллектуальные приложения не только лучше выявляют и предотвращают угрозы, но также автоматизируют расследование события и действия по реагированию.

Oracle — первый поставщик, встроивший такой уровень идентификации пользователей в свой облачный сервис, который интегрируется с другими механизмами безопасности для полной защиты гибридных сред. Сервис Oracle Identity Cloud Service (IDCS) является центром инфраструктуры безопасности, позволяя обеспечить нормативно-правовое соответствие, управление рисками и повысить защиту СУБД и приложений. Этот сервис упрощает развертывание таких приложений, как Office 365, Salesforce и Oracle Cloud Applications, а также обеспечивает синхронизацию учетных записей в облачном сервисе и локальных системах управления идентификацией на таких платформах, как Oracle Identity and Access Management и Microsoft Active Directory.

Сервис Oracle IDCS предоставляет различные административные возможности, включая управление пользователями, группами пользователей и приложениями, а также средства управления доступом, например единые учетные данные для входа в приложения, сильную аутентификацию и адаптивные политики с учетом рисков. Этот сервис работает во взаимодействии с сервисом Oracle Security Monitoring and Analytics Cloud Service для обнаружения, расследования и устранения большого диапазона угроз безопасности для всех локальных и облачных сред. Современная система Oracle SOC на основе идентификации включает анализ угроз безопасности, используя данные из открытых и коммерческих источников, белые и черные списки IP-адресов, репутацию устройств, известные уязвимости баз данных, геолокацию и т. д. SOC обеспечивает быстрое обнаружение, расследование и устранение большого диапазона угроз безопасности с помощью алгоритмов, способных выявлять шаблоны в данных. Система, которая становится все более интеллектуальной, может даже предсказать вероятность нарушений безопасности в будущем на основе данных за прошлые периоды.



Oracle Identity SOC — это первая в отрасли платформа на основе идентификации для центров мониторинга информационной безопасности.

Анализ на основе доверия

Хакеру относительно легко украсть учетные данные санкционированного пользователя и затем проникнуть в сеть под видом авторизованного сотрудника. Это может привести к подозрительным или аномальным действиям, которые отличаются от обычного поведения пользователя или его коллег. В этом случае система CASB подаст сигнал тревоги и применит более строгие ограничения для обеспечения безопасности — например, потребует двухфакторную аутентификацию для доступа к конкретному приложению. Кроме того, централизованная система идентификации дает возможность сотрудникам службы безопасности проверять, какие пользователи получают доступ к каким ресурсам и в какое время. Это позволяет выявлять ситуации, когда доступ уже не нужен пользователю, и устанавливать права доступа сотрудников к размещенным в облаке приложениям и права доступа третьих сторон к корпоративной инфраструктуре.

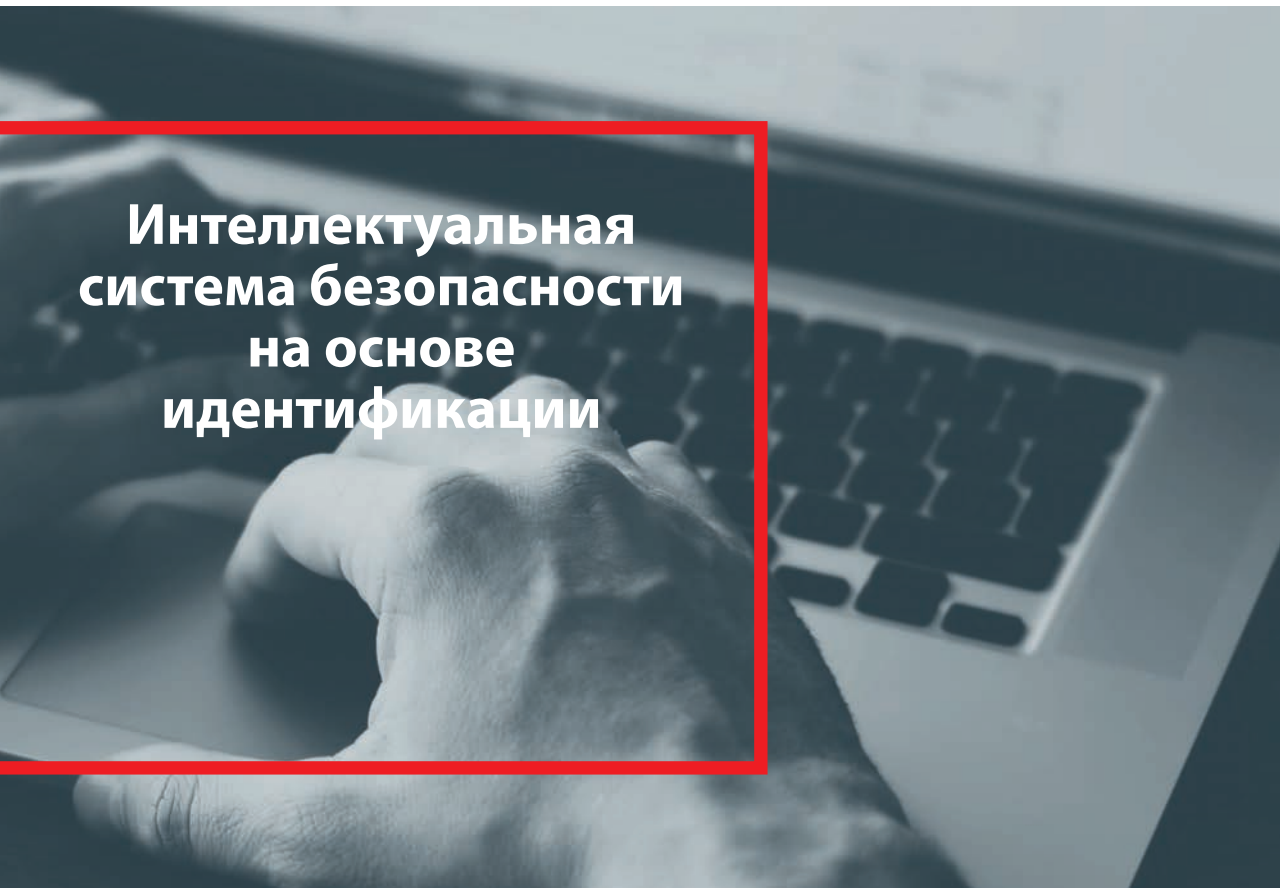
Oracle использует технологию машинного обучения для группировки пользователей на основе общих характеристик поведения (откуда они приходят, к каким внутренним ресурсам получают доступ, к каким облачным сервисам обращаются и в какое время суток работают). Это позволяет легко распознать аномальное поведение. Например, если специалист отдела кадров вдруг начинает вести себя как финансовый директор, это может быть индикатором украденной учетной записи или инсайдерской угрозы.

Автоматизация этого процесса необходима, учитывая количество тревожных оповещений и инцидентов в современной инфраструктуре. Например, специалист по SOC, пришедший утром на работу, может получить итоговый отчет, в котором сказано, что за выходные поступило 10 000 тревожных оповещений. Система безопасности автоматически приняла меры по 98 % этих оповещений (выдала сигналы тревоги, открыла заявки в службу поддержки и передала данные о возможных угрозах на другой уровень). Таким образом, специалисту остается проанализировать всего 200 оповещений.

Архитектурная интеграция

Как уже было показано, комплексная архитектура безопасности предполагает интеграцию людей, процессов и технологий через облачные инструменты, ориентированные на идентификацию. Чтобы связать все это воедино, требуются комплексные средства управления. Платформа Oracle Management Cloud включает механизм машинного обучения, который сопоставляет данные и обеспечивает управление из единого центра. Используются предварительно запрограммированные модели искусственного интеллекта, вам не нужен специалист в штате для программирования и обновления системы. Алгоритмы машинного обучения добавляют интеллект процессам DevOps и SOC. Например, один и тот же модуль системы безопасности обеспечивает нормативно-правовое соответствие и управление конфигурациями. Другие модули управляют данными и событиями безопасности (SIEM) и агрегируют их с помощью службы CASB. Платформа Oracle Management Cloud объединяет эти отдельные возможности в единой системе безопасности. Она идеальна для подразделений DevOps, внедряющих современные ИТ-методы, так как сопоставляет события, произошедшие в сети, приложениях и у пользователей, взаимодействующих с вашими системами.

Компания Oracle встроила технологию машинного обучения в платформу Oracle Management Cloud, что поможет вам справляться с угрозами безопасности в локальных и облачных средах. Такая основа для управления обеспечивает более продуктивное взаимодействие людей, процессов и технологии.



Интеллектуальная система безопасности на основе идентификации

Автоматическая киберзащита: будущее уже наступило

ИТ-специалисты ощущают потерю контроля по мере того, как традиционные рабочие нагрузки переносятся из хорошо защищенной, четко очерченной физической инфраструктуры в новые среды, где управлением инфраструктурой, приложениями и данными часто занимаются сторонние поставщики.

Сторонние поставщики облачных услуг не обладают доступом к данным своих клиентов, и их возможности мониторинга ограничены. Вот почему дальновидные руководители служб безопасности внедряют автоматические, интеллектуальные решения, действующие с учетом контекста. Это обеспечивает им эффективный контроль над возможными рисками для безопасности организации. Вместо пассивного мониторинга сети они создают проактивные системы безопасности, которые защищают пользователей, приложения, контент и данные. Что особенно важно, они могут решить, как согласованно применять инструменты безопасности в облачных и локальных средах.

Отсутствие эффективной защиты от внутренних и внешних угроз может отрицательно повлиять на вашу прибыль, торговую марку и рыночную стоимость ваших активов. Облачные службы и технологии машинного обучения повысят вашу готовность отражать атаки и дадут полное представление обо всей вашей ИТ-среде.

Благодаря Oracle ваш персонал обеспечит стабильную защиту и возможность оценки данных о событиях в реальном времени. Эта адаптивная система способна обучаться — например, узнавать, куда перемещаются сотрудники, какие устройства они используют и как изо дня в день меняются их среды.

Для организаций с развитой цифровой инфраструктурой очень важен эффективный анализ данных, связанных с безопасностью. Ручные процессы и технологии, основанные на правилах, уже не справляются с сегодняшними киберугрозами. Вам нужна автоматизированная контекстуальная технология машинного обучения для обнаружения и отражения известных и неизвестных угроз. Портфель интегрированных решений Oracle для обеспечения безопасности охватывает локальные и облачные среды. Он объединяет контекстуальную идентификацию как услугу, службы-посредники для безопасного доступа в облако, мониторинг и анализ безопасности, а также инструменты для настройки конфигурации и для обеспечения соответствия требованиям. И все это от одного поставщика, который поможет автоматизировать вашу киберзащиту и победить в кибервойне.

Для защиты от современных угроз необходимы технологии машинного обучения и облачные службы — новые средства информационной безопасности.

Узнать больше можно по следующим ссылкам:

Модернизация центра мониторинга информационной безопасности

Почему следует модернизировать системы управления и перенести их в облако

Официальный документ. Январь 2018 г.

Адаптивный анализ на основе машинного обучения: **будущее кибербезопасности**

Корпорация Oracle, головной офис
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Для международных запросов
Телефон: +1.650.506.7000
Факс: +1-650-506-7200

ORACLE