Решение по обеспечению безопасности Oracle Identity SOC

Идентификационно-центрическая безопасность для облачной эры

ORACLE

Oracle Identity SOC соотносит контекст идентификации с рисками для выявления рисков, связанных с безопасностью, и предоставляет ценную оперативную информацию для автоматического реагирования.

ПРЕИМУЩЕСТВА IDENTITY SOC

- Оперативные данные по инцидентам обеспечивают упреждающую защиту и послесобытийный анализ для определения первопричин.
- Устраняет бреши, с которыми не справляются сетецентрические инструменты.
- Расширяет возможности мониторинга без дополнительных ресурсов путем автоматизации анализа событий, расследования и реагирования.

ПОЧЕМУ СЕЙЧАС

- Передовые инструменты анализа данных обеспечивают потоковую передачу и анализ данных в реальном времени.
- Облачные решения необходимы, так как трафик обходит традиционные сетецентрические инструменты.
- Идентификация — это наилучший способ кросс-корреляции опасных действий при сложных атаках.

Введение

В наши дни атаки становятся все более изощренными. Угрозы нулевого дня разрастаются с беспрецедентной скоростью, что заставляет специалистов усомниться в эффективности выявления и предотвращения атак сигнатурными методами. Обнаружение аномалий единственным способом похоже на попытку найти иголку в стоге сена. Сегодняшние угрозы многовекторны и имеют множество точек проникновения, а этапы атаки разбиваются на сегменты меньшего размера, которые перекомпоновываются и выполняются. Атаки стали целенаправленными (в отличие от ранних неизбирательных атак), что делает информирование и идентификацию пользователей бесценными для выявления угроз. Возможность коррелировать аномальные события в сетях, приложениях и поведении пользователей имеет ключевое значение для раннего обнаружения и сдерживания атак.

Это ставит под сомнение эффективность сетецентрического подхода к защите, так как от имеющихся инструментов требуется защита данных и ресурсов способами, на которые они не способны. Идентификация стала мостом между мирами управления пользователями, приложениями и сетями. Именно контекст идентификации в сочетании с такими новыми технологиями, как машинное обучение, большие данные и передовая аналитика, позволяют специалистам по безопасности централизовать и нормализовать действия пользователей. Можно коррелировать и анализировать эти пользовательские действия и соотносить их с событиями облачных приложений, пользователей и сетей для выявления аномального и потенциально опасного поведения практически в реальном времени. И все это позволяет принимать превентивные меры для защиты от текущих и будущих атак на соответствующих направлениях.

Реализация нового сервиса Identity SOC

Традиционный операционный центр безопасности (SOC) предоставляет возможности управления устройствами и мониторинга для брандмауэров, систем защиты от вторжений, прокси-серверов и других технологий профилактики нарушений и защиты периметра. Наряду с управлением изменениями и обслуживанием устройств безопасности ведение журналов систем мониторинга и отслеживание событий выполнялись в основном через платформу управления информационной безопасностью и событиями безопасности (Security Information and Event Management, SIEM).

Identity SOC — это решение для выявления и автоматизации обработки событий на базе идентификационной и контекстной информации. Этот сервис обеспечивает необходимую гибкость для обнаружения современных угроз и постоянных атак и реагирования на них, а также предоставляет возможности обратной связи для адаптации и развития. Сервис Identity SOC призван защитить пользователей, приложения/API-интерфейсы, контент/данные и рабочие нагрузки.

Identity SOC использует оптимизированные панели управления и консоли оценки рисков для специалистов по безопасности, куда приходят данные от множества источников, таких как…

- Инструменты обеспечения безопасности, включая брандмауэры, IDS, IPS, веб-прокси, VPN, AV, DLP, DAM, WAF, сканеры уязвимостей
- Приложения и рабочие нагрузки, локальные и в облаке
- Инфраструктура, например IaaS, PaaS, EMM, ПО промежуточного слоя, СУБД, веб-серверы, гипервизоры и хосты (Windows, Linux и Unix)
- Сетевые инструменты, например маршрутизаторы, коммутаторы, DNS, DHCP и балансировщики нагрузки

ORACLE

Identity SOC использует современные средства анализа данных, такие как расширенная аналитика, машинное обучение и сложные инструменты обработки и анализа данных, которые обеспечивают идентификацию и расследование инцидентов практически в реальном времени. Поведенческая аналитика используется для выявления признаков подозрительного поведения, свидетельствующих об атаке. Моделирование путей атаки используется для предсказания пути, который может выбрать злоумышленник для повышения прав доступа. И наконец, Identity SOC обеспечивает автоматическую организацию (оркестровку) работы и реагирование. Двусторонняя интеграция делает сервис самовосстанавливающимся, что позволяет разным подразделениям взаимодействовать через продуманные сценарии и процессы.

Средства профилактики нарушений защищают лишь входную дверь, но для защиты всего вашего дома требуются инструменты обнаружения и реагирования.

Oracle представляет первый в мире сервис Identity SOC

Компания Oracle учла эти изменения в ландшафте безопасности и потребностях своих клиентов. Нам недостаточно просто защитить свое облако. Нашим клиентам нужны современные инструменты, которые обеспечат стабильную защиту в облачной и локальной средах. Согласно результатам исследования 2016 Right Scale, организации планируют использовать в среднем шесть (6) облачных сервисов для своих рабочих нагрузок. Как никогда требуется координированное управление безопасностью.

Oracle вкладывает значительные средства в первый в мире сервис Identity SOC. С тремя новыми облачными сервисами обеспечения безопасности, объединяющими несколько новых технологий в единый набор услуг. Интегрированные технологии включают: управление информационной безопасностью и событиями безопасности (SIEM), анализ поведения пользователей и сущностей (UEBA), управление идентификацией (IDM) и брокер безопасности доступа в облако (CASB). Каждый из этих новых сервисов может быть интегрирован с остальными вашими средствами безопасности, но вместе они обеспечат все преимущества Identity SOC с двусторонними средствами контроля и ценными оперативными данными.

Облачный сервис **Oracle Security Monitoring and Analytics (SMA)**, основанный на безопасной платформе больших данных Oracle Management Cloud, обеспечивает быстрое обнаружение, расследование и устранение широчайшего диапазона угроз безопасности как в облаке, так и локально.

Oracle Identity Cloud Service — это комплексная облачная платформа Oracle следующего поколения, предназначенная стать неотъемлемой частью системы безопасности организации и обеспечить современные средства идентификации для современных приложений.

Oracle Cloud Security Service — это ведущий брокер безопасности доступа в облако (CASB), который позволяет организациям защитить облачную инфраструктуру и данные, важные для бизнеса, при помощи объединенных средств обнаружения угроз, прогнозного анализа, управления конфигурацией безопасности, автоматического реагирования на угрозы и устранения угроз.

КОМПОНЕНТЫ IDENTITY SOC

- Оптимизированные панели управления и консоли оценки рисков
- Передовая аналитика, машинное обучение, интеллектуальная обработка и анализ данных
- Автоматическая оркестровка, реагирование на инциденты и самовосстановление

ПОЧЕМУ ORACLE

- Единственный поставщик, предлагающий SIEM, UEBA, CASB и IDM в едином интегрированном решении
- Безопасность во всем: лидер в области идентификации, больших данных, аналитики и безопасности данных
- Возможность для клиентов использовать средства защиты Oracle Public Cloud в своих системах

ORACLE

О компании WIND Hellas:

Головной офис:
Афины, Греция

Сотрудники: *1200*

Годовой доход:
4,5 млрд долл. США

Используемые решения:
Oracle CASB Cloud Service, Oracle Advanced Security

Oracle Cloud помогает компании WIND Hellas снизить риски и повысить соответствие Общему регламенту по защите данных ЕС (GDPR)

Мы выбрали облачный сервис Oracle Cloud Access Security Broker (CASB) и решение Oracle Advanced Security для минимизации рисков, достижения прозрачности операций и повышения контроля. Это позволило нам опережать возможные угрозы, применяя наши конфигурации безопасности в облачной среде и обеспечивая соответствие требованиям Общему регламенту по защите данных ЕС (GDPR) с минимальным ущербом для производительности.

— Димостенис Николопулос (Dimosthenis Nikolopoulos), директор по ИТ-операциям и разработке программ, WIND Hellas

О компании Telefonica Business Solutions:

Головной офис:
Мадрид, Испания

Сотрудники: *125 000*

Годовой доход:
Более 5 млрд долл. США

Используемые решения:
Oracle Identity and Access Management, Oracle Access Management Suit, Oracle Engineered Systems

Компания Telefonica Business Solutions повысила скорость адаптации пользователей на 10 % с помощью Oracle

Решение Oracle Identity and Access Management помогло нам снизить риски и улучшить нормативно-правовое соответствие. Мы быстро внедрили его для 10 000 наших пользователей (сотрудников и клиентов) с помощью сервиса Oracle Consulting и повысили скорость адаптации на 10 %. Это решение предоставляет возможность единого входа (SSO) в рабочие приложения.

— Гильермо Ланца (Guillermo Lanza), руководитель проекта, Telefonica Business Solutions

UBI Banca защищает свое облако с помощью облачного сервиса Oracle CASB

UBI Banca — это четвертая по величине итальянская коммерческая банковская группа с точки зрения рыночной капитализации с почти 2000 филиалов и более чем 22 000 сотрудников.

Растущие угрозы безопасности финансовых учреждений и новые нормативно-правовые требования побудили UBI Banca внедрить современную систему безопасности. Необходимо было минимизировать угрозы несанкционированного проникновения в облако и обеспечить соблюдение требований Генерального регламента ЕС о защите данных (GDPR) и Директивы по безопасности сети и информационных систем (NIS). Компания также хотела предоставить службам безопасности и операционным отделам полный обзор используемых облачных и локальных систем.

Успешное внедрение облачного сервиса Oracle CASB помогло компании UBI Banca на 50 % ускорить обнаружение новых угроз безопасности и на 80 % сократить время расследования случаев нарушения безопасности.

«Для многоканального, физического и цифрового преобразования нашего бизнеса требуется наивысший уровень безопасности, — говорит Фабио Джанотти (Fabio Gianotti), начальник службы безопасности, UBI Banca. — Мы реализуем гибридную стратегию операционных центров безопасности (SOC) на основе облачных технологий, и такой подход требует инновационных решений. Мы вложили средства в облачные сервисы безопасности Oracle, чтобы эффективно выявлять потенциальные угрозы и утечки данных, быстрее реагировать на них, а также обеспечить соответствие нормативно-правовым требованиям».

Узнать больше о современных решениях Oracle по обеспечению безопасности можно на странице cloud.oracle.com/security

Другие истории успеха заказчиков доступны на странице oracle.com/customers

СЛЕДИТЕ ЗА НАШИМИ НОВОСТЯМИ

blogs.oracle.com/oraclesecurity
facebook.com/oraclesecurity
twitter.com/oraclesecurity
oracle.com/security

142784, г. Москва,
п. Московский, Киевское шоссе, 22 км, д. 6, стр. 1

Телефон: +7 (495) 641 1400

Факс: +7 (495) 641 1414

ORACLE

Integrated Cloud Applications & Platform Services