Информзащита и Microsoft выведут на российский рынок виртуальный SOC

Издание: Anti-malware.ru

Автор: Олег Иванов

Компании «Информзащита» и Microsoft объявили о начале стратегического партнерства в области информационной безопасности, первым этапом которого станет вывод на российский рынок виртуального Security Operation Center (SOC) на базе Microsoft Azure Sentinel.

Опыт Microsoft в области создания решений по сервисной модели и собственная экосистема, включающая широкий спектр решений ИБ, в сочетании с одной из лучших на рынке экспертиз в области ИБ компании «Информзащита» позволят предложить российским заказчикам комплексные решения, в основе которых – управление системой ИБ предприятия из облачной среды. Кроме того, компании реализуют образовательную программу для российских компаний, позволяющую специалистам в области ИБ отработать самые сложные сценарии киберинцидентов. Также компании будут проводить совместные отраслевые мероприятия в области ИБ.

Сервис Microsoft Azure Sentinel – первая полностью интегрированная в облачную платформу Azure SIEM-система. Он позволяет автоматизировать рутинные задачи специалистов по кибербезопасности, освободив их время для решения приоритетных вопросов. Кроме того, применение технологий искусственного интеллекта (ИИ) позволяет снизить Alert Fatigue (медленное реагирование экспертов при слишком большом количестве сигналов тревоги) до 90%. Сервис обеспечивает защиту всей организации, обнаруживая и предотвращая угрозы до того, как они нанесут вред. Azure Sentinel использует неограниченные вычислительные мощности и масштабируемость облака Microsoft Azure для гарантии высокого уровня безопасности. Решение также собирает, объединяет и анализирует информацию со всего

предприятия – включая данные от пользователей, приложений и инфраструктуры как локально, так и в нескольких облаках.
Решение виртуального SOC включает в себя не только инновационную технологическую платформу, но и сервисы по мониторингу и реагированию на инциденты от экспертов Центра мониторинга киберугроз «Информзащиты» IZ:SOC. Все это позволит обнаружить кибератаки высокой категории сложности до того, как они глубоко проникнут в систему. Azure Sentinel поддерживает открытые стандарты, например, CEF, а также имеет широкую партнерскую сеть, включающую членов Microsoft Intelligent Security Association, таких как Cisco, Symantec, Fortinet, Palo Alto. Пользователи решения подтвердили, что оно сокращает время обнаружения киберугроз с нескольких часов до нескольких секунд. Решение также позволяет сотрудникам вносить собственные аналитические данные в систему и взаимодействовать с широким сообществом специалистов в области кибербезопасности.

*«Партнерство с Microsoft обеспечивает нам доступ к самым современным инструментам для защиты наших клиентов, позволяя находиться на самом острие развития современных технологий кибербезопасности. Возможности Microsoft в области искусственного интеллекта и облачных вычислений в сочетании с экспертизой сотрудников IZ:SOC дают эффективную синергию, направленную на повышение качества сервисов для наших заказчиков. «Информзащита» может осуществлять мониторинг объектов критической инфраструктуры, то есть наши заказчики в режиме одного окна могут получить сервисы, как обеспечивающие соответствие законодательству, так и направленные на защиту облачной части инфраструктуры», — говорит **Петр Ефимов**, генеральный директор АО НИП «Информзащита».*

*«Информационная безопасность является критически важным направлением для бизнеса любого размера. Согласно исследованию Juniper Research, ежегодный ущерб от деятельности киберпреступников будет расти каждый год в среднем на 11%, и к 2024 году превысит 5 трлн долларов. Российский рынок отвечает общемировой тенденции усложнения кибератак. Мы уверены, что объединение наших усилий с компанией «Информзащита», обладающей опытом реализации сложных проектов для крупного бизнеса, а также консалтинга в области ИБ, позволит укрепить информационную безопасность российских компаний. Для Microsoft в России трансформация партнерской экосистемы является стратегическим направлением, мы продолжаем развивать партнерства нового типа, поэтому начало работы с компанией «Информзащита» станет ярким примером такого сотрудничества», — говорит **Кристина Тихонова**, президент Microsoft в России.*

Подробнее: https://www.anti-malware.ru/news/2020-03-12-1447/32190