1. Рассмотреть российский цифровые платформы в выданной сфере.
2. Описать что относят к данной сфере.
3. Привести примеры платформ, относящихся к данной сфере.
4. Выделить плюсы и минусы с точки зрения пользователя.
5. Определить какие используются сквозные технологии.
6. Определить каким образом происходит монетизация.

С развитием информационных технологий проблема цифровой безопасности становится все более акутальной. Цифровые двойники, облачные сервисы хранения данных, электронные платежные системы и многое другое – все это вызывает острую нужду в системах цифровой безопасности.

Цифровая безопасность – это комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от вирусных атак и несанкционированного вмешательства. К данной сфере относятся: безопасность информации и цифровых данных; корректное хранение данных устройств в сети; обеспечение доступа к личным данным и денежным средствам посредством информационных устройств.

Большая часть решений в сфере цифровой безопасности являются иностранными, тем не менее на рынке есть и небольшое число российский предложений:

“Центр управления цифровой безопасностью” (сокращенно ЦУИБ) от ООО “Мультитек инжиниринг” (https://mte-cyber.by/services-and-solutions/cybersecurity-monitoring-and-management-center/) предлагает комплекс технологических решений для анализа и реагирования на инциденты информационной безопасности. Технологическим ядром ЦУИБ является связка SIEM (сбор, хранение и коррелированние данных) и SOAR (автоматизация работы с адимнистративными привеллегиями и реагированием на инциденты) систем. Монетизация производится за счет покупки системы заказичком, точные цены неизвестны, так как необходимо напрямую связаться с компанией. Плюсами платформы можно назвать: 1) превентивность реагирования за счет централизации функций детектирования и предотвращения, 2) контроль и обеспечение соответствия стандартам и законодательным актам всей системы информационной безопасности. Сквозные технологии применяемые в данной компании, как и почти во всех в данной сфере – big data и искуственный интеллект. Единственным минусом можно назвать то, что использование платформы предполагает делегирование доступа к особо важным элементам работы бизнеса чужой компании.

“Гарда Аналитика” (https://gardatech.ru/produkty/ap/) – это другая российская платформа информационной и экономической безопасности. Система работает за автоматизации процессов обнаружения отклонений в поведении сотрудников и систем, за счет непрерывного сбора и анализа поступающих данных. Монетизация проводится аналогичным образом с ЦУИБ от ООО “Мультитек инжиниринг”. Главным плюсом платформы является применение сквозных технологий Big Data. Другим плюсом является то, что платформа устанавливается на объекте заказчика и чувствительные данные не передаются в облако. Возможным минусом может являться новизна платформы, из-за чего она может быть не настолько отполированна как другие.

“R‑Vision TDP” от R-Vision (https://rvision.ru/). Данная цифровая платформа предлагает комплекс технологий цифровой имитации элементов ИТ-инфраструктуры для обнаружения злоумышленников. Ее плюсы таковы: обнаружение атак, которые невозможно детектировать другими средствами (APT, 0-day и другие угрозы), снижение скорости горизонтального перемещения киберпреступника внутри сети и искажение периметра ложными элементами ИТ-инфраструктуры. Система монетизируется аналогичным образом с предыдущими. Данная платформа является одной из лучших на рынке и выделить определенные минусы у нее сложно. Любые минусы решаются решениями из экосистемы R-Vision окружающей платформу.

Другими примерами платформ, относящихся к данной сфере будут: ThreatStream – SaaS (доступ к готовому програмному обеспечению по подписке) платформа анализа информации об угрозах включающая более 140 каналов с открытым исходным кодом и позволяющая легко включать коммерческие каналы через Anomali APP Store; ThreatConnect – платформа, предоставляющая возможность автоматизировать агрегирование источников информации об угрозах, особо подчеркивается возможность кастомизации рабочего опыта и группа профессиональных аналитиков стоящих ; “Мозг” от Panda - интеллектуальная платформа информационной безопасности, разработанная для устранения современных угроз, главной ее особенностью является контекстный интеллект, позволяющий выявлять закономерности поведения вредоносных программ и генерировать стратегии защиты.