Команда «Cybercell» компании Azercell - вице-чемпион соревнования «Кибервойна», прошедшего в рамках CIDC-2023

26 и 27 октября 2023 года в Бакинском конгресс-центре проходил киберфестиваль «Critical Infrastructure Defense Challenge» (CIDC-2023). Мероприятие, организованное Государственной службой специальной связи и информационной безопасности и Службой государственной безопасности Азербайджана, стало важной вехой в сфере кибербезопасности Азербайджана. Впервые в Азербайджане в виртуальной войне с моделированием кибератак приняли участие сотрудники отделов информационной безопасности государственных организаций, образовательных учреждений, телекоммуникационных компаний и банков. В рамках конкурса «Кибервойна» команда «Cybercell», в состав которой вошли сотрудники Департамента безопасности Azercell Вусал Гасанов, Амираслан Гулиев, Джавид Джаббарлы, Ахмед Гаджылы и Чингиз Балабеков, завоевала титул вице-чемпиона. Всего к участию в конкурсе была допущена 41 команда, представлявшая государственные и частные учреждения, относящиеся к категории критической инфраструктуры, 20 из которых вышли в финал. В то же время сотрудник Департамента безопасности Исмаил Эйюб занял первое место в личном зачете конкурса «Захват Флага», опередив 135 других участников. О том, как проходили соревнования и какой импульс придаст проведение подобных мероприятий развитию сферы кибербезопасности в Азербайджане мы поговорили с Исмаилом Эйюбом.

- Насколько был высок уровень ваших соперников на CIDC-2023?

- Среди участников соревнований были как специалисты со значитель-

ным опытом работы в сфере кибербезопасности, так и в IT в целом. Их опыт и компетенции подтверждены международными сертификатами в данной области, что лишний раз говорит о профессионализме представителей большинства команд. Наряду со столь опытными профессионалами, конечно же, участие в конкурсе принимали и студенты вузов нашей страны, которые имеют немалый опыт в подобных соревнованиях. Также стоит отметить, что конкурс «Захват Флага» (Capture the Flag - CTF), который проводился в рамках CIDC-2023, - очень специфическое соревнование. Для участия в нем нужен особый метод мышления и постоянная практика, приобретение которой немыслимо без участия в похожих соревнованиях, а также без изучения вопросов, встречающихся на международных соревнованиях формата «Захват Флага». Принимая во внимание все эти факторы, можно с уверенностью сказать, что уровень конкуренции на соревновании был очень высоким.

«Мы очень гордимся выдающимися результатами нашей команды «Cybercell» в конкурсе CIDC-2023. Это достижение подчеркивает нашу приверженность защите критической инфраструктуры от киберугроз и укрепляет позиции Azercell как ведущего оператора связи. Мы также поздравляем нашего сотрудника Исмаила Эйюба, занявшего первое место в индивидуальных соревнованиях, и желаем ему новых успехов», - руководитель Департамента безопасности Azercell Фуад Сафаров.

- Какие задания необходимо было выполнить в рамках конкурса «Захват Флага»?

- Задания на соревнованиях формата «Захват Флага» обычно состоят из нескольких категорий. Проверяются не только знания участника в той или иной конкретной области кибербезопасности и его хакерских способностей, а целиком в IT-сфере. Например, на данном конкретном соревновании были такие категории заданий, как «Crypto», «Web», «Reverse Engineering», «OSINT» и другие. Каждая из них включала от 3 до 6 вопросов, оцениваемых

Сотрудник Департамента безопасности «Azercell Telecom» Исмаил Эйюб

по сложности в пределах от 750 до 5000 баллов. Суммарно же было чуть больше 20 вопросов во всех категориях, в которых можно было набрать 41000 баллов. Например, в заданиях категории «Web» необходимо было найти уязвимость в предоставленных веб-приложениях и с их помощью прочитать «флаг» из текстового файла на сервере, на котором данное приложение существовало. В заданиях категории «OSINT» нужно было найти «флаги», используя предоставленные короткие сведения о человеке или команде людей. И никаких дополнительных сведений о том, где и как найти «флаги» не предоставлялось, поэтому рассчитывать приходилось только на свой опыт и интуицию.

- Можете оценить уровень сложности заданий?

- Все зависит от самого задания и уровня подготовки участника. Были задания, которые при достаточном уровне знаний можно было решить за считанные минуты. Например, в одной из категорий было задание, в котором предоставлялось некое мобильное приложение в формате «.apk». Чтобы найти «флаг», стоило лишь прочитать все текстовые слова в исходном коде приложения с помощью соответствующей команды в терминале операционной системы Linux. Однако, были и довольно трудные задания, на решения которых ушел не один час. Одно из таких заданий так и осталось незавершенным мною. Уже по результатам соревнования я узнал у одного из администраторов соревнования, что мое решение было верным и стоило лишь найти нужный «флаг». В условии того задания сообщались имя, фамилия, прозвище, кличка питомца и дата рождения некоего разработчика, а также то, что путь к «флагу» лежит в некоем комментарии. Связав комментарии и разработку приложений, я подумал, что названный разработчик мог поделиться своим мнением о чем-то на популярной среди специалистов данной профессии платформе GitHub. С помощью специальной утилиты, используя предоставленные данные о человеке, я вывел возможный список имен пользователей и начал их проверять их существование на названной платформе. Один из возможных пользователей действительно существовал и его аккаунт был создан лишь 11 часов назад. Перейдя на страницу пользователя в субплатформе GitHub Gist, я нашел несколько файлов, которыми он поделился с сообществом. Среди файлов был также один особенный, в котором разработчик поделился своими любимыми местами на картах. Список состоял из строк формата «слово1.слово2.слово3», где каждая из трех частей, казалось бы, была случайным словом из английского словаря. Однако, при поиске сервисов карт, связанных с тремя словами, я наткнулся на «what3words.com», который превращал координаты на карте в набор из трех слов для простоты запоминания. Осуществив поиск по всем 24 местам из списка в данном сервисе, я нашел места от Колизея в Риме до Девичьей Башни в Баку. Чтобы найти «флаг», нужно было найти те же места на Картах Google и прочитать отзывы по ним за последние несколько дней. Так что, в принципе, при достаточной подготовке можно было бы справиться со всеми заданиями и набрать максимальные 41000 баллов.

- Сколько всего человек принимало участие в конкурсе «Захват Флага» на CIDC-2023?

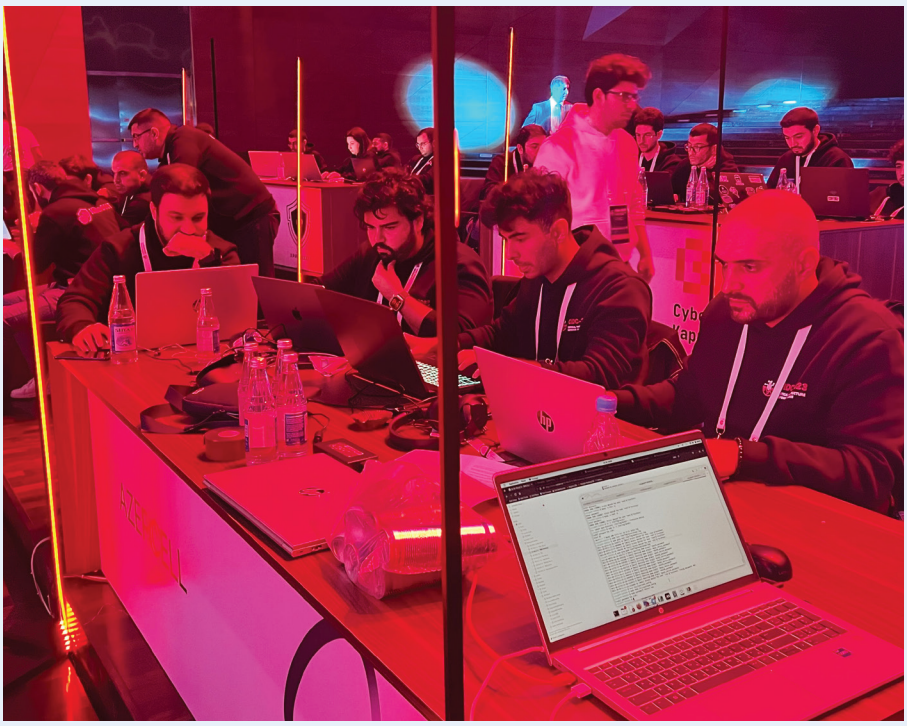
- CIDC-2023 стал одним из крупнейших мероприятий, посвященных вопросам обеспечения кибербезопасности и развитию этой темы в нашей стране. Наряду с основными соревнованиями «Кибервойна» и «Захват Флага», в рамках «Critical Infrastructure Defense Challenge» также были организованы обучающие семинары по разным темам в данной сфере. И участники всех возможных активностей на CIDC-2023 могли проверить свои знания, приняв участие в соревновании по «Захвату Флага». В итоге их общее число достигло 136 человек.

- А каким было командное соревнование «Кибервойна» и с какими трудностями пришлось столкнуться команде Azercell на пути к тому, чтобы стать призером данного конкурса?

- «Кибервойна» - одно из двух главных соревнований финала CIDC-2023. Соревнование состояло из двух отборочных этапов и гранд-финала. Участие в первом отборочном этапе приняла 41 команда. Все они представляли самые разные компании и организации, являющиеся частью критической инфраструктуры Азербайджана. В состав каждой команды входило по 5 человек. Во второй отборочный этап прошла 31 команда. Здесь проходили состязания на самый быстрый и точный ответ на вопрос, что напоминало формат конкурса «Захват Флага». По итогам отборочных этапов 20 лучших команд получили право на участие в гранд-финале, который проходил с 26 по 27 октября, став самым значимым мероприятием года в сфере кибербезопасности. Главной целью финального этапа для каждой команды было устранение уязвимостей в предоставленных семи системах, а также обустройство инфраструктуры для их защиты от потенциальных атак. После двух дней подготовки на созданные инфраструктуры были совершены умышленные атаки, в результате которых и оценивался уровень их подготовки к отражению реальных атак. Наша команда в течение нескольких недель тщательно изучала самые различные методы устранения уязвимостей во множестве популярных систем, а также методы быстрой конфигурации «с нуля» вероятных систем для обеспечения кибербезопасности. Упорный труд и усердие привели нас к победе.

- Чем формат соревнований в рамках CIDC-2023 отличался от проводимых ранее хакатонов по теме кибербезопасности?

- CIDC-2023 - уникальное соревнование для Азербайджана во многих аспектах.



Как командный, так и индивидуальные турниры были проведены на самом высоком уровне. Для достижения высоких результатов были привлечены многие компании, а также специалисты и эксперты из Турции и Азербайджана. Кроме того, постоянная поддержка, которая оказывается мероприятиям подобного формата со стороны государства также способствовала развитию столь уникального опыта в истории нашей страны. Одной из главных отличительных черт командного турнира стал его фокус на обеспечении комплексной безопасности, нежели на атаках на уже построенные системы, тогда как ранее все подобные соревнования проходили именно во втором формате. Одновременно с этим сам факт предоставления всем 20 командам-финалистам современных и распространенных в профессиональной сфере технологий и программ для обеспечения безопасности стал отличительной чертой CIDC-2023.

- Как вы оцениваете общую организацию CIDC-2023 и что вы хотели бы увидеть на подобных мероприятиях в Азербайджане в будущем?

- Однозначно можно сказать, что мероприятие и соревнования в его рамках были проведены на достойном уровне, что очень порадовало нас не только как участников, но и как профессионалов в данной сфере. Условия проведения состязаний позволили увидеть, как представители большого числа компаний и государственных организаций собрались на одной площадке, чтобы в дружественной атмосфере конкурировать на новом и постоянно развивающемся направлении развития нашей страны. Сам факт подписания Господином Президентом «Стратегии Азербайджанской Республики по информационной безопасности и кибербезопасности на 2023-2027 годы» является залогом будущего успеха нашей Родины в данной сфере. По нашему мнению, формат CIDC-2023 является самым подходящим на данном этапе развития рынка кибербезопасности в Азербайджане. В качестве ускорения роста в этой сфере хотелось бы, чтобы к участию в подобных мероприятиях на постоянной основе привлекалось больше зарубежных специалистов, например, из братской Турции, для совместного проведения подобных турниров и взаимного обмена опытом.

- Какую пользу участие в подобных мероприятиях может принести для вашей компании и для страны в общем?

- Плюсов очень много. Если говорить о стране в целом, то такие соревнования привлекают большое количество молодых и мотивированных людей, заинтересованных в сфере кибербезопасности, и создают для них условия для демонстрации своих навыков на весь Азербайджан. Также такие мероприятия привлекают к участию в них крупнейшие локальные компании и холдинги, например, Azercell, которые заинтересованы в усилении своих команд по информационной и кибербезопасности. А подобные соревнования как раз и являются катализатором навыков и способностей наших специалистов в данной сфере.

- А какое место занимают вопросы обеспечения кибербезопасности непосредственно в Azercell?

- Само понятие кибербезопасности в Azercell достаточно новое, впрочем, как и для всей нашей страны. Однако, благодаря постоянной поддержке, которую мы ощущаем в компании на всех уровнях, начиная от руководителя нашего Департамента и заканчивая президентом Azercell, эта сфера в компании развивается достаточно интенсивно. Всего за 2 года мы добились огромных успехов, что вызывает невероятное чувство гордости от совершенного прогресса. Мы видим, как кибербезопасность становится одной из решающих сфер деятельности Azercell, одновременно оправдывая вложенные в ее развитие средства и усилия. Доказательством тому, кстати, и служит наш успех на крупнейшем мероприятии по кибербезопасности в истории страны - CIDC-2023!