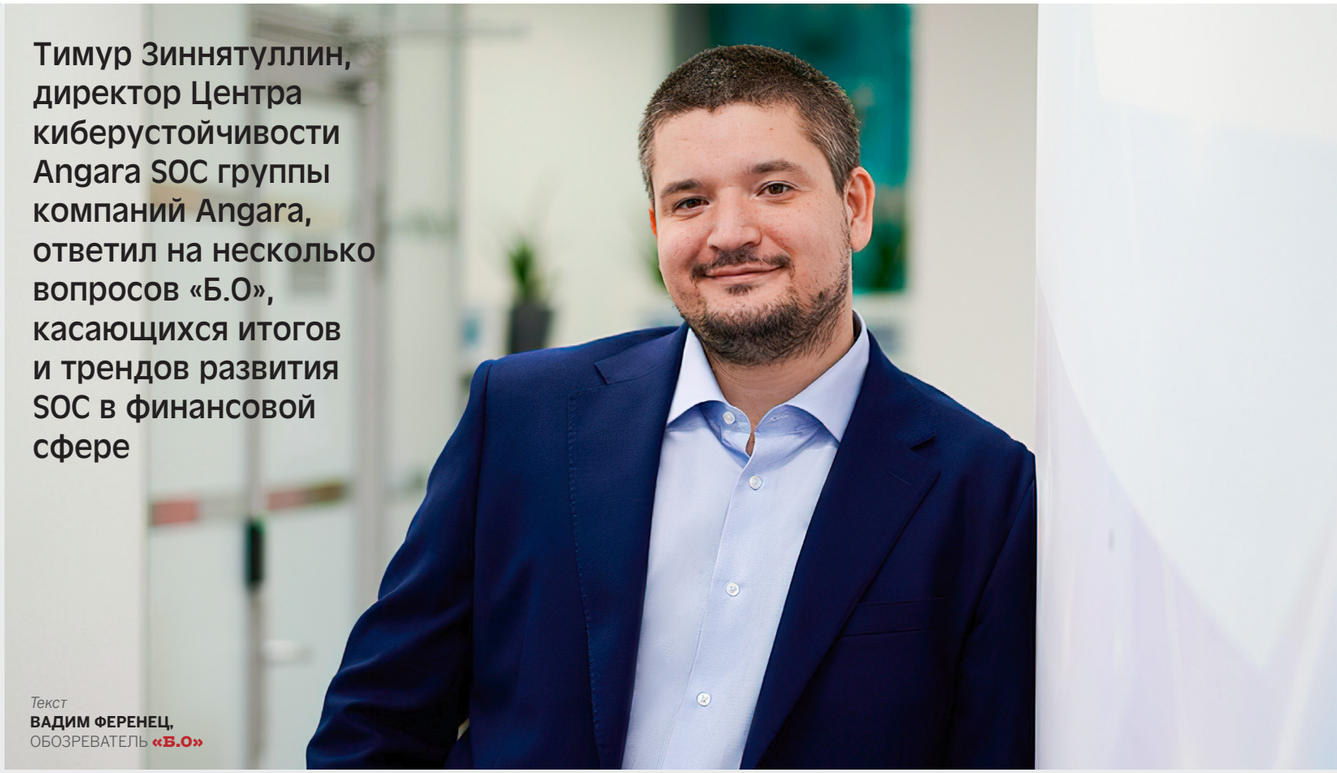
Тимур Зиннятуллин (Angara Security): Главное — не подвести



Тимур Зиннятуллин, директор Центра киберустойчивости Angara SOC группы компаний Angara, ответил на несколько вопросов «Б.О», касающихся итогов и трендов развития SOC в финансовой сфере

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Тимур, по вашей оценке, какие векторы развития SOC в финансовом секторе будут превалировать в 2023 году?

— Финансовые институты по всему миру, включая Россию, — это те организации, в которых научились неплохо управлять операционными рисками, в частности рисками ИБ и IT. Оперриски напрямую влияют на прибыльность, а значит, на дивиденды акционеров, в числе которых может быть и государство. Кроме того, отрасль в значительной мере зарегулирована — начиная с отечественного ГОСТа и заканчивая зарубежным PCI DSS.

Применительно к сегменту SOC (security operations centers) в составе ИБ-инфраструктуры банка, страховой компании и тому подобных это означает, что его роль в снижении потенциального ущерба от реализации инцидентов операционного риска начинает прорабатываться на самых ранних стадиях развития компаний. Уже на этих этапах, как правило, процессы управления рисками в банках находятся на более зрелом уровне по сравнению с предприятиями из других отраслей экономики, что положительно сказывается на оптимальной архитектуре SOC, а также на определении метрик эффективности его работы.

Однако, несмотря на то что специалистам для включения в арсенал SOC доступно множество превентивных мер и средств защиты, например статических и динамических анализаторов, а также на то, что растет количество источников данных об угрозах и их форматах, на мой взгляд, существует ключевая проблема, которая задает вектор развития сегмента. Я имею в виду голод экспертизы (не кадровый голод), который усугубляется острой потребностью в квалифицированных кадрах.

— Эта проблема возникла сейчас или у нее есть предыстория? Как ее решать?

— Проблема экспертизы существовала и ранее, сейчас же она стала гораздо более актуальной. Я имею в виду, например, то, что уровню культуры ИБ в целом и роли концепции security by design в частности уделялось меньше внимания, чем она заслуживала. Ситуацию можно описать как «запущенность ряда ИБ-процессов». Это продолжалось довольно долго, и вот сейчас, по моему мнению, проблема попала в ряд приоритетов для решения, что не может не радовать. Я полагаю, что выправление ситуации будет связано с реализацией трех взаимосвязанных ключевых направлений.

Во-первых, это автоматизация различных стадий обработки информации, включая анализ подозрений на инциденты и их обработку с использованием различных классов инструментов — от привычных уже SOAR до новейших математических моделей и нейронных сетей.

Во-вторых, это повышение квалификации персонала. Решение этой проблемы неизбежно, иначе адекватно противостоять тем угрозам, с которыми мы столкнулись в 2022 году, невозможно.

Наконец, третий вектор — импортозамещение. Здесь есть нюанс: какими бы классными решениями не располагал тот или иной вендор (отечественный или из дружественной страны), финальный результат будет зависеть от исполнителей на местах. Экспертиза вендора ограничивается функциональными возможностями его продуктов. Она хороша в рамках написания сигнатур или чего-то под свой контекст, но встраивание вендорских решений в процессы конкретного банка с учетом тонкостей его операционной деятельности находится за рамками экспертизы вендоров. Это же касается и необдуманного перехода на open source, для этого требуется созреть. Поэтому в рамках импортозамещения необходимо и развитие партнерской сети, и повышение квалификации кадров.

— Какие метрики эффективности SOC сегодня актуальны?

— Это один из самых больных вопросов, ведь если служба ИБ отлично справляется со своим функционалом и не допускает серьезных инцидентов, то у топ-менеджмента неизбежно появится вопрос: «А за что именно мы платим службе безопасности?».

Лучшей мировой практикой, как мне представляется, является стандартный договор SLA (Service Level Agreement) — соглашение об уровне сервиса, согласно которому партнеры несут финансовую ответственность в рамках своих полномочий.

Опыт ГК Angara говорит о том, что с менеджментом заказчика лучше всего общаться в метриках его собственной бизнес-эффективности, а еще лучше — в финансовых терминах. Чтобы перевести ИБ-показатели на язык, понятный бизнесу, мы развиваем направление Security Intelligence, позволяющее дать оценку эффективности средств защиты информации в рамках тех или иных ИБ-процессов с учетом опыта профессиональных сообществ по классической методике SMART. По нашим оценкам, этот подход используется уже примерно в 20% компаний из пула наших клиентов. Потребность в данной экспертизе начинает проявляться на рынке, это совершенно очевидно.

— Чем организациям из финансового сектора может быть полезна экспертиза ГК Angara?

— В 2021 году на Национальном киберполигоне нам повезло, и мы заняли второе место. В 2022 году наша команда пентеста там же взяла первое место. Хоть я и сказал «повезло», на самом деле — это закономерный результат многочисленных внутренних спринтов, заключающихся в периодических, но при этом неожиданных тестах нашей собственной инфраструктуры и проверке качества услуг, которые мы оказываем. Команды Red Team (команды «нападения», организующие кибератаки на IT-инфраструктуру компании, чтобы выявить ее слабые места), проводящие внешний и внутренний мониторинг, непрерывно оттачивают свои инструменты и методики, которые потом используются в реальных пентестах. Но самое интересное то, что пятилетний опыт спринтов позволяет вырабатывать достаточно интересные методики, уникальные для нашего рынка. Поэтому первое, чем мы можем быть полезны рынку, — это уникальный контент.

Второе — наши знания по техникам закрепления злоумышленников в IT-инфраструктуре. Зачастую при услугах пентеста или анализе защищенности команды «нападающих» по причине различных факторов (сроков или границ проектов) пропускают этот этап. Мы же, наоборот, расширяем свои навыки в этой нише и выработали механизмы выявления и противодействия более 30 техникам закрепления. Весь этот контент внедрен в наш собственный коммерческий SOC. Кроме того, мы активно делимся с заказчиками экспертизой и переносим полученный опыт в их внутренние процессы.

Наконец, у нас в Центре работают более 60 человек, настоящих профессионалов, в развитие интеллектуального потенциала которых вкладывается немало времени и усилий. Это весомый аргумент в нашу пользу.

— Какова сегодня роль ИИ в SOC? Поверили вы в него?

— В 2022 году произошло множество событий, которые помимо всего прочего изменили мое отношение к ИИ. Наверное, до зимы прошлого года я крайне скептически относился даже к разговорам об этой технологии применительно к ИБ, потому что не видел ни одного эффективного, коммерчески рационального метода его применения.

Резкий рост SOC привел к необходимости искать пути автоматизации первичных стадий обработки инцидентов — агрегации, обогащения, закрытия части инцидентов автоматом и так далее — для того, чтобы не отвлекать на это аналитиков. В итоге у нас на сегодня около 20% всех поступающих инцидентов закрывается IRP-системой. Наверное, это потолок тех технологий, которые мы применили.

Мы поняли, что потенциал у ИИ есть, об этом же говорит опыт наших коллег из других компаний. Поэтому сейчас мы «ищем себя», пробуем разные модели, в частности для реализации анализа подозрений на инциденты по направлению защиты web, так как веб-канал является источником огромного количества аналитического материала. Есть и другие планы, но всему свое время. Б.О