Максим Степченков (RuSIEM): Банки лучше готовы к развертыванию собственного SOC, чем они сами думают

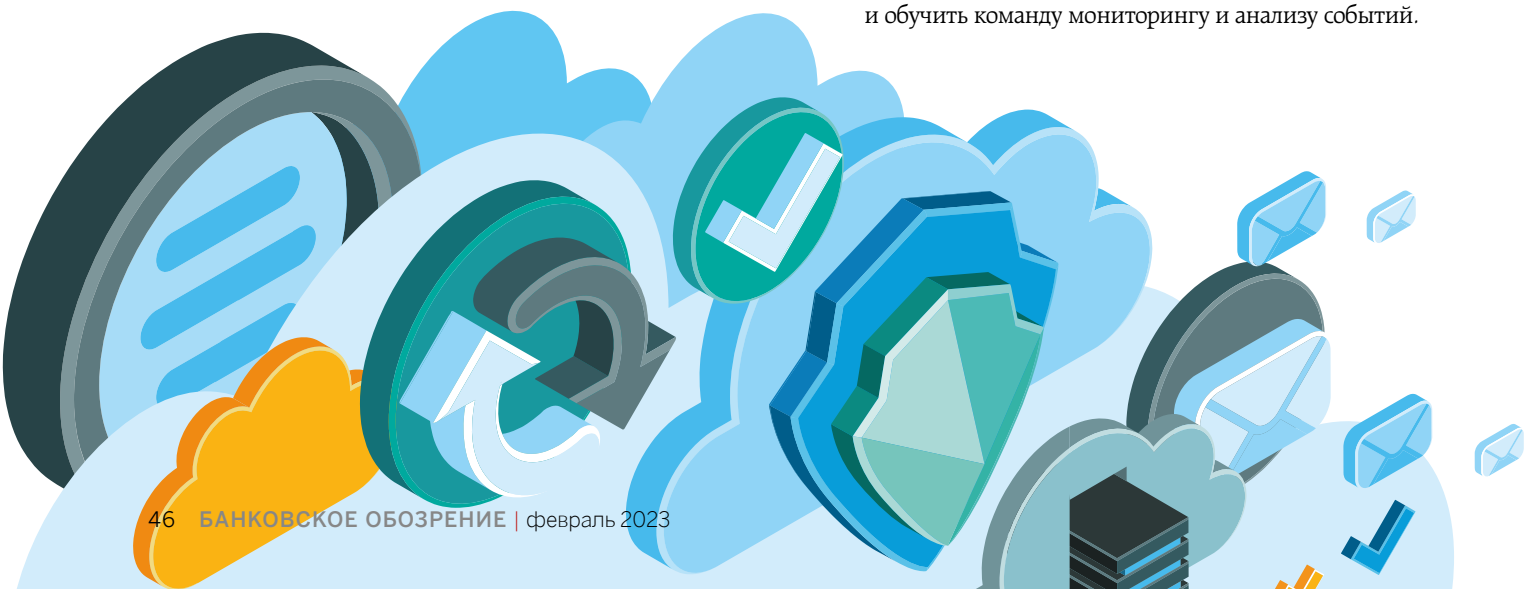
Совладелец компании RuSIEM Максим Степченков перечислил условия, при которых система мониторинга и обнаружения инцидентов может трансформироваться в Security Operation Center

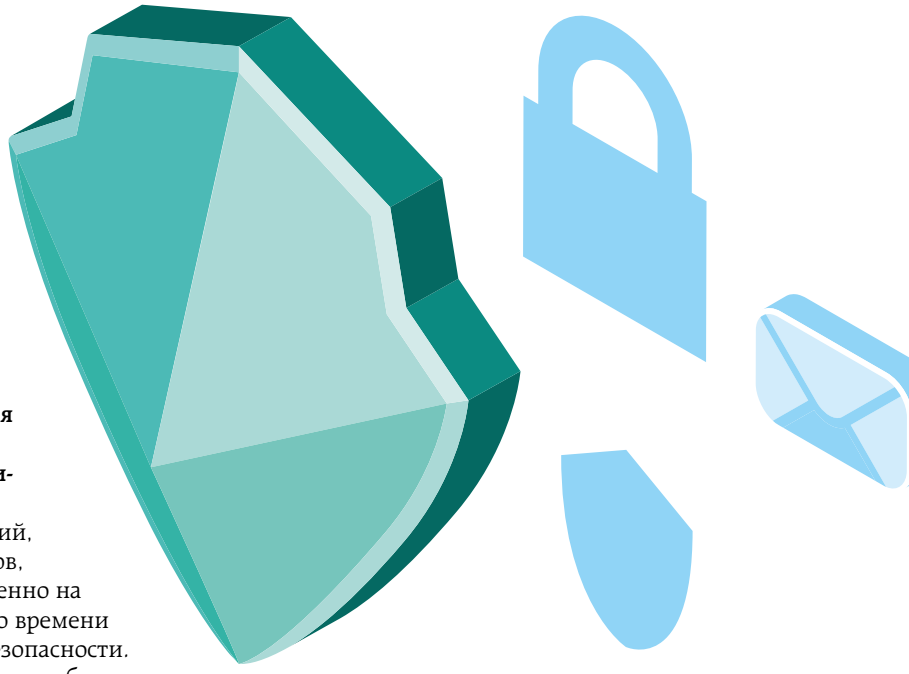
Текст
ЕЛЕНА ПОКАТАЕВА,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Максим, для какого круга финансовых компаний построение SOC является действительно эффективным решением? Какие могут быть альтернативы?

— Альтернативой может быть услуга SOC, которую финансовая компания получает на рынке от внешнего поставщика. Однако такой сценарий содержит риск попадания заказчика в некую технологическую зависимость от конкретного провайдера услуги SOC. Скажем, если пути заказчика и поставщика сервисов разойдутся, коммерческий SOC оставит на своей стороне все данные о мониторинге информационной безопасности. Чтобы исключить этот риск, финансовым организациям имеет смысл реализовать гибридную схему — развернуть на своей стороне SIEM-систему, а обработку и реагирование на события информационной безопасности возложить на исполнителя.

Для банков покрупнее — скажем, из топ-100 по размеру активов — более оправданным шагом будет создание собственного SOC. Обычно это банки с большим количеством клиентов, они не только имеют дело с корпоративными заемщиками, но и ведут достаточно заметный розничный бизнес. В таких банках исторически сложилось так, что функция ИБ становится бизнес-критичной. Взломы и утечки могут повлиять на непрерывность бизнеса. В таких банках почти всегда есть сильная ИБ-команда с опытом реагирования на угрозы. Они готовы к созданию собственного SOC лучше, чем они сами думают. Три четверти технологий и ресурсов для этого у них уже есть. Наш опыт показывает, что иногда достаточно просто добавить SIEM и обучить команду мониторингу и анализу событий.





— Какие положительные и отрицательные последствия могут быть, если защищать не всю инфраструктуру, а только критические бизнес-процессы?
— О положительных последствиях здесь говорить не приходится. Да, возможно, таким образом компания сможет сэкономить бюджет, но экономия получится ограниченной, локальной. Это все равно что зимой ездить на летних шинах. Какое-то время вы сможете удерживать контроль над автомобилем, но рано или поздно все закончится плачевно.

— Может ли связка SOC/SIEM заменить сегодня все остальные ИБ-системы: DLP, UEBA, DCAP, а также антифрод-системы на уровне бизнес-систем или по транзакциям по счетам?
— Точно нет. SIEM анализирует журналы событий, которые ведутся различными типами источников, в том числе и DLP-, UEBA-, DCAP-системами. Именно на основании анализа событий в режиме реального времени SIEM выявляет инциденты информационной безопасности. Если же SIEM будет нечего анализировать (на вход не будут поданы данные о событиях), ни о каком выявлении инцидентов не сможет быть и речи.

С другой стороны, на базе SIEM реализуемы и антифрод, и DCAP, и частично UEBA. Но это возможность, а не основная функция.

— Как оценить полноту покрытия SOC?
— Поскольку абсолютной защиты не существует, при попытке оценить полноту имеет смысл исходить из наших представлений о том, что мы готовы допустить, а что не готовы. Мы не готовы к тому, чтобы обычный пентест закончился успехом атакующей стороны. Мы понимаем, что все стандартные/общеизвестные уязвимости должны быть выявлены. Мы должны принять тот факт, что злоумышленник может воспользоваться новой уязвимостью, но при этом задача SOC — максимально быстро выявить подозрительную активность и предпринять соответствующие меры. Вместе с тем очевидно, что сервисами SOC в первую очередь должны быть накрыты те участки инфраструктуры, которые обеспечивают функционирование критически важных бизнес-процессов. От более важных фрагментов IT-ландшафта следует идти к менее важным и в итоге охватить средствами SOC всю инфраструктуру. При этом, конечно, не забывать, что для адекватной оценки степени защищенности разумно регулярно использовать независимые аудиты и статистику.

— Какие технологии сейчас используются в SOC? Как минимизировать при этом человеческий фактор?
— Ядром SOC, как правило, выступает SIEM, так как решения именно этого класса позволяют анализировать огромные объемы данных в режиме реального времени. Для минимизации человеческого фактора при расследовании и реагировании на инциденты очень подходят IRP - и SOAR-системы. Они позволяют автоматизировать процесс реагирования на инциденты и предоставляют наборы плейбуков (шаблонов с рекомендациями по реагированию). Эти системы серьезно облегчают работу команды реагирования на инциденты и вместе с тем снижают влияние на итоговый результат действий, допущенных ИБ-специалистом по невнимательности или в силу ограниченности времени на реагирование. Это тот самый человеческий фактор.

— Каковы возможности развития риск-ориентированного подхода к решению задач в области ИБ и страхования киберрисков?
— Утопия. По крайней мере — до момента появления четких общепринятых практик в рамках риск-ориентированного подхода. Пока такая перспектива не просматривается. Кроме того, страхование не решит проблему защищенности компаний от кибератак но снизит мотивацию страхователей инвестировать в информационную безопасность.

— Какова сейчас ситуация с подготовкой и удержанием кадров?
— Кадровый вопрос всегда комплексный. Его решение с точки зрения любой компании в какой-то степени зависит от состояния рынка труда, однако именно эта зависимость открывает новые возможности для организаций, намеревающихся создавать свой SOC. Первым делом имеет смысл повысить зарплаты специалистам информационной безопасности по крайней мере до уровня «классических» айтишников, чтобы подняться над медианным уровнем вознаграждения. Причем, если это сделать на опережение, есть шанс собрать с рынка грамотных специалистов раньше, чем это сделает кто-то другой.

Второе — взять курс на автоматизацию мониторинга и противодействия инцидентам, причем в рамках конкретного стека технологий и решений, чтобы не распылять ресурсы.

Третье — не просто выращивать ИБ-специалистов внутри организации, а показать им траектории их профессионального и зарплатного роста, чтобы мотивировать оставаться с конкретной компанией так долго, как это будет им интересно. Б.О