SOC с нуля

Особенности построения центра мониторинга в региональном финансовом учреждении

Текст
АЛЕКСАНДР КИРИЙ,
РУКОВОДИТЕЛЬ ОТДЕЛА МОНИТОРИНГА
И АНАЛИЗА ЗАЩИЩЕННОСТИ «КСБ-СОФТ»

Высокая вероятность рисков взлома и остановки бизнес-процессов из-за роста числа сложных атак на инфраструктуру коммерческих предприятий и государственных учреждений в 2022 году показала важность обеспечения защиты их информационных ресурсов. Поэтому сегодня для своевременного реагирования на атаки руководители организаций все больше интересуются практической безопасностью, в частности вопросами построения центра мониторинга и реагирования на компьютерные инциденты (SOC).

Основной причиной создания SOC для региональных финансовых учреждений становится необходимость:

- сокращения негативных последствий: утечек данных, их удаления или модификации, сбоя или отказа в работе программного обеспечения;
- снижения финансовых рисков: вывода денег со счетов, остановки деятельности, штрафов;
- соответствия законодательным требованиям.

Особенностью региональных финансовых учреждений субъектов РФ является дефицит либо полное отсутствие ИБ-специалистов для осуществления работ по информационной безопасности. Кроме того, в подобных учреждениях за многолетнюю историю их существования выстроена сложная инфраструктура, состоящая из архитектурно разрозненных, внедренных с разными целями информационных систем, а также установленных и настроенных без учета общей концепции информационной безопасности средств защиты информации.

Необходимо учитывать эти особенности при построении SOC для корректного предотвращения несанкционированного доступа к информации и обеспечения стабильности финансовых процессов.

Учитывая перечисленное выше, а также результаты аудитов с выявлением наиболее критичных узлов в инфраструктуре организаций, мы пришли к выводу, что для региональных финансовых учреждений подходящим решением является модель аутсорсингового SOC.

При построении SOC особое значение на первом этапе имеет корректная настройка центрального компонента системы мониторинга, позволяющей аккумулировать поток событий и проводить их анализ с объединением по группам в инциденты ИБ. Затем для контроля периметра внедряются системы, отвечающие за захват и анализ сетевого трафика. Кроме того, на АРМ и серверах проводится настройка для передачи информации о событиях ИБ в центральный компонент.

Наиболее критичными инцидентами для финансовых учреждений в практике нашей компании оказались целенаправленные фишинговые рассылки с вредоносными вложениями на почтовые адреса среднего и высшего руководящего звена, что могло бы стать причиной финансовых и репутационных потерь или невозможности выполнения текущих задач организацией, в том числе по планированию бюджета. Однако благодаря установленным средствам защиты и своевременному реагированию специалистов SOC атаки на инфраструктуру финансовых учреждений были остановлены.

Анализируя динамику инцидентов и их типы, мы можем сделать вывод о том, что снижение их количества возможно только при своевременном выполнении сотрудниками учреждений рекомендаций специалистов SOC. Там, где рекомендации выполняются несвоевременно либо вовсе не выполняются, отмечается стабильный рост компьютерных инцидентов.

Таким образом, практика исполнения ИБ-проектов показывает, что наиболее эффективным решением при обеспечении практической безопасности в небольших/региональных финансовых учреждениях является внедрение модели аутсорсингового SOC. Б.О