Практические аспекты построения SOC

Широко распространенные на сегодняшний день решения класса SIEM позволяют решить задачу автоматизации процесса сбора и анализа событий безопасности. Однако само по себе внедрение системы мониторинга не дает возможность автоматически перейти от SIEM к полноценному ситуационному центру SOC, позволяющему выполнять непрерывное оперативное управление инцидентами информационной безопасности. Почему так происходит, какие трудности возникают при переходе от SIEM к SOC и как их преодолеть, рассказали эксперты компаний "ДиалогНаука" и HPE.

Поскольку инфраструктура обеспечения безопасности расширяется и эволюционирует, эксперты в корпоративной безопасности сталкиваются со все более серьезными и сложными угрозами. В частности, все большей проблемой становятся внутренние угрозы. Так, согласно оценкам, озвученным архитектором решений ИБ компании HPE Евгением Афониным, среднее по миру время обнаружения проникновений в корпоративную ИКТ-инфраструктуру составляет 243 дня.

Количество угроз ИБ постоянно растет, появляются новые уязвимости и способы атак, современные ИТ-системы становятся все сложнее, а число их пользователей увеличивается с каждым днем. В таких условиях необходимо стремиться к минимизации времени между выявлением инцидента и реагированием на него.

Традиционные решения оповещают организации о подозрительных действиях согласно заранее определенным признакам инцидента, однако к тому моменту, когда событие исследуют и будут предприняты соответствующие меры в зависимости от ситуации, злоумышленники уже нанесут серьезный ущерб. Согласно недавнему исследованию, проведенному компанией Verizon, 82% всех выявленных инцидентов безопасности показали, что деятельность злоумышленников можно было отследить через системные файлы журналов безопасности.

Однако сегодня руководители организаций все чаще обнаруживают, что традиционные системы защиты больше не способны справляться с постоянно изменяющимися угрозами. И хотя решения для управления корпоративной безопасностью, такие как SIEM, выполняют свою основную функцию, все чаще они оказываются беспомощны перед современными угрозами, когда признаки инцидента заранее предсказать невозможно, так как российскими пользователями инструментов SIEM применяются готовые, разработанные вендорами правила и отчеты.

Следующим за внедрением и эксплуатацией систем SIEM логическим этапом повышения киберзащищенности для компаний является этап построения собственного SOC или обращение за услугами SOC к внешним провайдерам соответствующих услуг.

Согласно статистике, собранной специалистами HPE, только 25% организаций смогли организовать эффективную работу своих SOC. По оценкам Gartner, причины столь невысокого показателя успешности заключаются в организационных аспектах внедрения и эксплуатации.

Ксения Засецкая, старший консультант отдела консалтинга компании "ДиалогНаука", рекомендует перед принятием решения о постройке собственного SOC оценить уровень зрелости процессов ИБ своей компании и готовность к построению ситуационного центра. Для организации SOC в компании уже должны существовать основополагающие процессы ИБ, которые лягут в его основу. В некоторых случаях, возможно, будет правильнее обратиться к аутсорсинговым компаниям, предоставляющим услуги внешних SOC. ●