SOS, который защищает

В начале этого года ДП «ЭС ЭНД ТИ УКРАИНА» сообщила об успешном внедрении своей комплексной системы информационной безопасности. О ней мы побеседовали с генеральным директором компании Юрием Михайловичем Лисецким.

Юрий Михайлович, в начале этого года компания «ЭС ЭНД ТИ УКРАИНА» публично анонсировала успешное внедрение комплексной системы информационной безопасности (ИБ) для одного из заказчиков. Расскажите о ней подробнее.

В 2018 году наша компания разработала Security Operation System — SOS. Система интегрируется в ИТ-инфраструктуру (ИТИ) организации и обеспечивает сбор и обработку событий безопасности, анализ инцидентов и реакцию на развивающиеся и успешные атаки, а также выполнение процедур для минимизации ущерба от этих атак.

Основной целью внедрения SOS является создание инструмента, который позволит ИБ-команде эффективно обнаруживать как попытки атак и атаки в развитии, так и действия злоумышленников в ИТИ. Система дает возможность не только получать обогащенную информацию для расследования инцидентов безопасности, но и организовывать процесс самого расследования в соответствии с разработанными политиками и правилами.

Для достижения этой цели SOS успешно решает следующие задачи: сбор и корреляция информации об ИТ-процессах, журналов событий, параметров трафика и пр.; предоставление собранной и обработанной информации в контексте расследования; организация процесса расследования и, наконец, применение полученных знаний для внесения изменений в систему ИБ.

Очевидно, что для эффективной работы системы необходимо анализировать события не только на периметре, но также и внутри ИТИ.

Техническая и процессная компоненты SOS не могут быть эффективными без грамотной ИБ-команды. Поэтому мы предлагаем адаптированное для конкретного заказчика штатное расписание, распределенное по ролям, и требования к компетенции и навыкам для каждой роли. Мы также подготовили программу обучения для каждой роли, начиная от базовых знаний. На время обучения и становления ИБ-команды мы готовы обеспечивать поддержку и сопровождение SOS.

SOS представляет собой комплекс программно-аппаратных средств: аналитическое ядро системы и средства борьбы с киберугрозами (обычно его элементы уже присутствуют в ИТИ), которые предоставляют данные для ядра SOS. Ядро системы занимается сбором, корреляцией, обработкой данных, проведением анализа, выявлением инцидентов и сопровождением расследований. Основной элемент ядра SOS — аналитическая платформа Splunk Enterprise, интегрированная с набором дополнительных программных модулей.

Нашими специалистами для ИТИ каждого заказчика подбираются и разрабатываются подходящие для конкретных условий правила сбора, корреляции и анализа событий.

Название Security Operation System, однозначно, перекликается с общепринятым Security Operation Center. Почему вы выбрали свое название?

В общих чертах SOS, конечно же, наследует концепцию Security Operation Center (SOC). В упрощенном виде SOC — это технические средства и команда, задача которой обнаруживать, анализировать, уведомлять о возникновении, реагировать и предотвращать инциденты информационной безопасности.

При внедрении нашей системы мы больше внимания уделяем процессам подбора, настройки и интеграции технических средств ИБ, включая те, что уже есть у заказчика и могут использоваться без изменений либо достраиваться или модернизироваться. Мы стремимся довести эффективность технического комплекса до максимально возможной в каждом конкретном случае. Осуществляется не просто работа над центром системы ИБ, под которым обычно и понимается SOC, но мы ее изначально перестраиваем и модернизируем таким образом, чтобы обеспечить максимальную защищенность заказчика и получить максимум информации для

анализа ядром системы. Отсюда акцент на слово «система» в названии нашего решения.

Решение уровня SOC является весьма сложным, а конкуренция на рынке велика. Как Вы подошли к осознанию своевременности решения SOS?

Я бы назвал три взаимосвязанных причины: две внешних и одну внутреннюю. Во-первых, за последние годы участились атаки на государственные и коммерческие организации в Украине. Во-вторых, у наших корпоративных заказчиков в последнее время появилось понимание, что абсолютно надежную систему кибербезопасности создать невозможно, поэтому очень важно быстро обнаружить взлом и расследовать инцидент. На этом фоне возникла острая необходимость в модернизации и наращивании своих возможностей по ИБ. И в-третьих, некоторое время назад мы ясно осознали, что существовавших на тот момент у нас опыта и экспертизы в области ИБ скоро станет не хватать для качественного ответа на современные вызовы. Поэтому мы предприняли ряд действий по повышению квалификации и увеличению ИБ-команды, а также разработке своих решений по ИБ. Все это привело к синергетическому объединению профессионалов, процессов и программно-аппаратного комплекса Security Operation System и созданию нашей методологии — триединого подхода к обеспечению ИБ заказчиков.

Результаты пилотных проектов и внедрений SOS подтвердили правильность и эффективность такого подхода.

Почему вы открыто заявили о решении лишь в этом году, а не в 2018-м, когда оно было разработано?

Я скажу больше — истоки решения уходят в 2017 год. Тогда не в последнюю очередь благодаря WannaCry, а потом и Petya, мы увидели большое количество случаев беспомощности унаследованной концепции кибербезопасности с акцентом только на защиту периметра, а также неготовность к Zero-day атакам. Поэтому мы форсировали работу и в 2018 году вышли на уровень, который позволил проводить успешные пилотные проекты, а затем и внедрения.

Мы не спешили с публичностью в силу специфики вопроса. Мы хотели накопить положительный опыт и прийти к полной уверенности в том, что наша система управления ИБ сможет эффективно решать сложные задачи. Недавнее успешное внедрение для одной из государственных силовых структур стало для нас подобным подтверждением.

«ИБ как услуга» vs «ИБ онсайт»: почему вы выбрали вторую модель?

Круг наших заказчиков в большей степени ориентирован на вторую модель. Помимо корпоративных стандартов и законодательных требований, свою роль здесь сыграли ее преимущества. Прежде всего, своя система безопасности всегда настроена намного лучше на процессы в защищаемой ИТИ и на контекстное понимание инцидентов внутри сети. Кроме того, те, с кем мы работаем, могут выделить финансовые и организационные ресурсы на формирование собственного SOC и не хотят, чтобы внутренняя информация, касающаяся безопасности, циркулировала во внешней сети, пусть и партнерской. С персоналом ситуация сложнее — все знают о дефиците кадров для ИБ — и здесь на помощь приходит наша методология.

Почему вы выбрали продукты Splunk в качестве основы решения?

У «ЭС ЭНД ТИ УКРАИНА» есть опыт разработки собственного корреляционного движка для решений поддержки операционных процессов (OSS), мы также внедряли, эксплуатировали или тестировали довольно много продуктов класса SIEM, корреляционных движков и аналитических систем.

Мы провели тщательный анализ и сравнение программно-аппаратных комплексов ядра. Для нас было важно гибко адаптировать систему под различных заказчиков; легко ее масштабировать; эффективно интегрировать с различными компонентами существующей ИТИ; иметь возможность построить на этой же платформе систему управления процессом расследования инцидентов; объединять ее с другими аналитическими системами, минимизировать финансовые затраты. Именно по этим критериям выбор был сделан в пользу аналитической платформы Splunk.

Расскажите подробнее о процедуре внедрения SOS.

Внедрение SOS производится в таком порядке: обследование, выяснение наиболее опасных векторов атак и наиболее уязвимых ИТ-активов, определение необходимости и объема модернизации сети заказчика, развертывание программно-аппаратного комплекса аналитики и корреляции и подключение его к существующим источникам событий и отчетов, адаптация набора правил обработки и корреляции/создание новых правил, создание и адаптация процедур и политик для ИБ-команды, удаленная поддержка системы (от уровня второй-третьей линии до уровня аутсорсинга).

Для внедрения SOS необходимо наличие минимального набора средств ИБ: NGFW, система предотвращения/обнаружения вторжений, система защиты оконечных точек, инфраструктурные серверы. Более эффективным SOS делает наличие в ИТИ систем поиска уязвимостей (Vulnerability Manager) и приманок-ловушек (Deception/HoneyPot).

По вопросам сотрудничества обращаться в **ДП «ЭС ЭНД ТИ УКРАИНА»** *— 03142, Киев, Проспект Академика Палладина, 44А, а также по тел. +380 (44) 238–63–88, e-mail: info@snt.ua, сайт www.snt.ua*