SOC на аутсорсинге

Задача центра управления безопасностью — помочь справиться с объемом данных об угрозах.

Михал Гарцаж, технический руководитель Cisco Security Operations

Компания Cisco занимается как построением центров безопасности, так и предоставлением SOC-услуг по модели аутсорсинга. Об особенностях этого бизнеса и о технологиях, которые в нем используются, журналу «СиБ» рассказал Михал Гарцаж, технический руководитель Cisco Security Operations Center (Краков, Польша).

— Чем SOC отличается от традиционного мониторинга и контроля безопасности, действующих на предприятиях, в частности, с помощью SIEM?

— Инструменты Security Information and Event Management (SIEM) используются для сбора информации об инцидентах безопасности. Они обеспечивают в реальном времени анализ предупреждений (alerts), создаваемых приложениями и сетевым оборудованием. В SOC мы предлагаем SIEM как услугу. Мы сопоставляем информацию об инцидентах, поступающую из всех доступных источников, чтобы определить, указывают ли они на реальное нарушение безопасности или только на угрозу. Объем данных, подлежащих анализу для определения нарушения, настолько велик, что бизнес не может сделать это самостоятельно. И вот здесь важна роль SOC.

— Есть ли международные стандарты, которые определяют правила построения SOC?

— Таких стандартов нет. Существуют нормы — например, ISO 2700, или лучшие практики-рекомендации, такие как ITIL, которых мы придерживаемся в нашей работе. Но нет стандартов и норм, указывающих, как следует строить SOC. У Cisco есть свои внутренние ноу-хау и лучшие практики. Кроме того, несколько лет назад мы выпустили OpenSOC — эталонную техническую архитектуру и набор лучших практик по созданию SOC на основе элементов с открытым исходным кодом.

— Как давно Cisco предоставляет услуги SOC и какие решения использует?

— Подразделение, положившее начало SOC, было открыто в 2004 году с приобретением NetSolve — поставщика услуг по управлению удаленными сетями и ИТ-инфраструктурой для предприятий и сервис-провайдеров. NetSolve удаленно контролировала, диагностировала и решала целый ряд проблем сетевой и ИТ-инфраструктуры, связанных с LAN/WAN, а также IP-связью и безопасностью. Также SOC использует технологию Cisco Active Threat Analytics (ATA), которая позволяет обнаруживать угрозы безопасности и реагировать на них. С ее помощью можно анализировать сетевой трафик клиентов, оценивать телеметрию безопасности и применять данные наблюдений, полученные от аналитической службы Cisco Talos. Инженеры SOC обеспечивают как экспертный мониторинг киберугроз, так и удаленные операции для устройств безопасности.

— Возможно ли размещение такого центра на территории клиента, или речь идет только о виртуальном SOC?

— Некоторые компании владеют собственными SOC. Это в основном крупные предприятия, работающие с конфиденциальными данными, которые не позволяют внешним подрядчикам получать доступ к ним. Однако аутсорсинговые услуги становятся все более популярным способом управления безопасностью на предприятиях по всему миру. Причиной тому являются масштабы киберугроз и экспоненциальный рост числа атак, что в сочетании с нехваткой квалифицированных кадров в сфере безопасности затрудняет обеспечение полноценной защиты предприятия. Аутсорсинг услуг — разумный способ решения этой проблемы.

В последние годы мы часто наблюдаем гибридную модель SOC, когда клиенты управляют безопасностью наиболее критичных систем самостоятельно, внутри компании, а часть функций отдают на аутсорсинг. Компетенции двух структур строго разделены, но они обмениваются всей необходимой информацией, чтобы полностью защитить инфраструктуру клиента и другие активы.

— В каких направлениях будут развиваться технологии SOC в ближайшем будущем?

— По моему мнению, мы будем наблюдать дальнейшее развитие таких направлений, как автоматизация, «Интернет вещей» и промышленные сети, машинное обучение. Изменения в этих областях полностью преобразуют привычную работу SOC.

У специалистов SOC будет больше времени, чтобы сосредоточиться на стратегических аспектах. Передовые технологии будут продолжать указывать на потенциальные проблемы, но только высококвалифицированный специалист по расследованию угроз сможет дать взвешенную оценку и принять правильное решение.

Подготовил **Василий ТКАЧЕНКО,**
СиБ