УДК 004.05

Р. В. Стрельников

SOC. НЕЭФФЕКТИВНОСТЬ ВНЕДРЕНИЯ

Проанализированы основные недостатки и проблемы внедрения ситуационного центра мониторинга информационной безопасности (Security Operation Center).

The paper analyzes the main shortcomings and problems of implementing a situational center for monitoring information security (Security Operation Center).

Ключевые слова: SOC, центр мониторинга информационной безопасности, информационная безопасность.

Keywords: SOC, information security monitoring center, information security.

Введение

В настоящее время практически все крупные организации различных структур обеспокоены современными угрозами информационной безопасности. Такой интерес вызван прежде всего постоянно совершенствующимися атаками на информационные ресурсы и потребностью в современном инструменте противодействия им.

По статистике, злоумышленники могут находиться в сети компании до момента их обнаружения более 180 дней. Это приводит к большим финансовым потерям. Так, за 2018 г. в результате атаки вируса-шифровальщика пострадало множество крупных мировых межнациональных компаний. Только в прошлом году был ряд скандалов, связанных с утечкой конфиденциальной информации, персональных данных и промышленным шпионажем. В этом году таких утечек стало в несколько раз больше. Поэтому актуальным в настоящее время является поиск решений, позволяющих минимизировать подобные риски.

Одно из них — построение эффективного ситуационного центра мониторинга информационной безопасности *Security Operation Center* (SOC), представляющего собой совокупность программно-аппаратных средств, персонала и процессов. Они предназначены для централизованного сбора и анализа информации о событиях и инцидентах информационной безопасности (ИБ), поступающих из различных источников ИТ-инфраструктуры [1]. Действительно, SOC является одним из ключевых компонентов подразделения информационной безопасности любой организации. Он нацелен на мониторинг, выявление и оперативное реагирование на инциденты и, как следствие, снижение возможных последствий, к которым тот или иной инцидент может привести.

Необходимость создания SOC

Любая крупная организация рано или поздно сталкивается с необходимостью создания SOC. Предпосылки создания центра реагирования, как правило, следующие:

— отсутствие единой картины происходящего в инфраструктуре;

— невозможность эффективно применять текущие меры защиты;

— отсроченное реагирование на инциденты ИБ;

— разрозненные центры ответственности;

— отсутствие сквозного процесса между подразделениями информационных технологий (ИТ) и ИБ;

— большое количество активных средств защиты информации;

— постоянно развивающаяся инфраструктура;

— требования стандартов PCI DSS и ISO 27001.

Но далеко не все компании готовы внедрить у себя SOC по следующим причинам:

— недостаток персонала и опыта, поскольку ИБ не является для компании профильным направлением;

— отсутствие процессов ИБ или несоответствие бизнес-задачам компании;

— отсутствие достаточного финансирования, направленного на организацию SOC;

— отсутствие базовых средств ИБ (межсетевых экранов, настроек аутентификации, централизованного ведения журналов мониторинга).

При этом минимальными требованиями, позволяющими компании перейти к реализации SOC и получить преимущество на рынке, являются:

— наличие базовых средств ИБ;

— наличие возможности и системы сбора журналов безопасности с оборудования;

— поддержка топ-менеджмента;

— подход к ИБ с точки зрения риска.

Для круглосуточного функционирования операционного центра необходимы несколько линий поддержки, программное обеспечение (SIEM-решения, платформа распознавания инцидентов, система учета инцидентов, сканеры уязвимостей и т. п.), мощности (система виртуализации, серверы, система хранения данных), отдельный сегмент для SOC (для снижения риска несанкционированного доступа к информации и другим угрозам).

Вместе с тем несомненными преимуществами, которые предоставляет операционный центр, являются:

— снижение рисков ИБ за счет своевременного обнаружения и обработки инцидентов;

— повышение уровня управления средствами безопасности и защищенности информационной системы;

— снижение рисков отказов системы и времени восстановления системы;

— возможность дальнейшего развития системы управления и контроля ИБ.

Эффективность внедрения центра

Однако не каждый SOC будет эффективен в работе, ведь организация центра — часто нетривиальная задача, которая к тому же выступает компромиссным решением между финансированием, кадровым вопросом, разработкой регламента взаимодействия и современных технологий ИБ. Качество и эффективность работы SOC обеспечивается конвейерным подходом в организации труда, строгой специализацией ответственных сотрудников, автоматизацией рутинных задач и тесным взаимодействием с остальными подразделениями — как в части реагирования на инциденты, так и в части определения актуальных задач ИБ. Такая организация центра позволяет обеспечить стабильное качество работы сотрудников по выявлению и реагированию на инциденты ИБ, четко понимать структуру инвестиционных и операционных затрат с учетом заданного уровня качества, а также иметь возможность их обоснования перед руководством.

В качестве базовой платформы для организации центра, как правило, выступает система мониторинга событий ИБ (SIEM — Security Information and Event Management). При этом необходимо понимать, что SOC не равен SIEM. SOC может существовать и без SIEM, правда, в ущерб эффективности и зрелости применяемых методов. Но обычно SIEM является сердцем центра реагирования, его ядром.

Часто бывает и так, что после организации операционного центра и довольно приличного финансирования SOC остается в подвешенном состоянии. А ведь его сотрудникам приходится ежедневно контактировать с большим количеством подразделений, и без поддержки руководства и четко определенной цели обеспечить эффективную работу по расследованию инцидентов невозможно. При этом основная ставка делается на технические решения. Это самая частая ошибка в работе SOC: бюджет тратится на внедрение технических решений, что приводит к недостаточной квалификации и количеству специалистов. Большинство современных угроз требует серьезной квалификации аналитика, а также высокого уровня организации работы по расследованию инцидентов.

Ошибки создания SOC

К другим ошибкам по созданию и организации работы SOC можно отнести следующие.

1. Отход от правила «от простого к сложному». Проблемы с решением базовых задач ИБ обязательно приводят к затруднениям при решении задач более высокого уровня. Управление информационными

активами, корреляция кадровой информации, категоризация информационных активов — все это ключевая информация при расследовании инцидентов.

2. Решение второстепенных задач оказывает негативное влияние на результаты работы ситуационного центра. Обеспечение формального соответствия требованиям регуляторов или стандартам не всегда приводит к существенному повышению уровня защищенности.

3. Финансирование SOC зачастую заканчивается на этапе внедрения. Обеспечения ресурсами их повседневной работы зачастую недостаточно, однако совершенно необходимо для эффективной деятельности.

4. Ошибка подбора режима работы сотрудников, а также слабая подготовка аналитиков SOC. Некомпетентный персонал и персонал с недостаточной подготовленностью снижает время реакции на инцидент.

5. Неправильный выбор расписания работы сотрудников, неэффективная организация труда ведут к увеличенному количеству ошибок. Особенно это заметно при режиме работы SOC в режиме 24/7 (половина времени работы центра). Так, основные особенности ночной смены:

а) биологические часы сотрудников не перестраиваются, даже если постоянно работать в ночную смену;

б) потеря аппетита, проблемы с пищеварением и кардиологией — серьезные последствия для здоровья;

в) напряжение и стрессовые ситуации после дневного сна приводят к снижению внимательности, возрастанию времени реакции, ухудшению памяти;

г) выпадение из социума, социальные изменения и проблемы в семье.

6. Главный недостаток — то, что не существует эффективной автоматизации SOC. Все программные комплексы приходится дополнительно настраивать или дописывать. Однако при грамотном подходе автоматизация центра позволяет минимизировать человеческий фактор на первом уровне поддержки.

Перспективы развития

ИТ-ландшафт продолжает стремительно развиваться, вместе с ним растет и объем событий в области информационных и защитных систем. В большинстве организаций сегодня человек не в состоянии анализировать этот поток событий и выбирать из него информацию, на которую стоит обратить внимание. Если говорить об инциденте, ценно не только его оперативное выявление, но и скорость реакции. SOC как раз позволяет автоматизировать процесс реагирования на инциденты ИБ. Именно поэтому ответом на современные реалии является SOC. Организациям нужна эффективная операционная структура, которая в состоянии выполнять достаточно трудоемкие операции ИБ: мониторинг и анализ событий, реагирование на инциденты, threat hunting и т.д.

В последнее время активная законодательная деятельность в области ИБ требует внедрения тех или иных мер информационной безопасности. Нагрузка на сотрудников ИБ возросла многократно. Остро стоит

вопрос недостатка квалифицированных специалистов, который серьезно ограничивает выполнение полного объема мероприятий, направленных на соблюдение законодательных требований и решений прикладных задач ИБ. Эти тенденции рождают серьезный спрос на автоматизацию рутинных операций и услуги сервисов по ИБ.

При этом предотвращение возможных инцидентов безопасности, включающее деятельность по повышению осведомленности персонала и контроль уязвимостей ИТ-инфраструктуры, будет основным вектором развития SOC еще несколько лет.

Список литературы

1. *Muniz J., McIntyre G., Al Fardan N.* Security Operations Center: Building, Operating, and Maintaining your SOC // Cisco Press. Nov 2, 2015. URL: http://www.ciscopress.com/store/security-operations-center-building-operating-and-maintaining-9780134052076 (дата обращения: 11.10.2019).

Об авторе

Роман Владимирович Стрельников — заместитель директора — руководитель ГАУ КО «Калининградский государственный научно-исследовательский центр информационной и технической безопасности», Россия.

E-mail: strelnikov.roman@gmail.com

The author

Roman V. Strelnikov, Deputy Director, Head of the Kaliningrad State Research Center of Information and Technical Security, Russia.

E-mail: strelnikov.roman@gmail.com