DOI 10.52209/1609-1825_2021_2_168 УДК 004.054

Основы построения SOC

[1]***КОБЛАНОВ Нурбек Бахытулы,*** *магистрант, n_koblanov@kbtu.kz,*
[1]***СУЛИЕВ Расим Ниязович,*** *PhD, ассоциированный профессор, декан, r.suliev@kbtu.kz,*
[1]*Казахстанско-Британский технический университет, Казахстан, 050000, Алматы, ул. Толе би, 59,*
**автор-корреспондент.*

Аннотация. *Сегодня вопросами построения Security Operation Center (SOC) интересуются практически все представители отечественной экономики: от страховых компаний и банков до крупных промышленных предприятий. Такой интерес вызван прежде всего постоянно совершенствующимися атаками и потребностью в современном инструменте противодействия им. Действительно, SOC является одним из ключевых компонентов подразделения информационной безопасности любой организации. В первую очередь он нацелен на мониторинг, детектирование и оперативную реакцию на инциденты, и, как следствие, на сокращение ущерба и финансовых потерь, к которым тот или иной инцидент может привести. Как расставить приоритеты, с чего стоит начать построение SOC для достижения конкретных результатов в короткие сроки? Цель статьи – дать полученные на собственном опыте рекомендации при построении SOC.*

Ключевые слова: *SOC, on-premise, out-source, ИТ, ИБ, оценка рисков.*

Введение

Построение своего SOC (Security Operation Center, центр наблюдения и оперативного реагирования на происшествия ИБ) – масштабный проект для любой организации. Первичный шаг планирования – это фундамент, от которого зависит, как верно будет работать механизм идентификации и реагирования на происшествия ИБ.

Основываясь на практическом опыте сотворения своего коммерческого SOC (АО Казтелепорт), строительства SOC у наших заказчиков, также на межгосударственных методологиях и практиках, мы поведаем о первых важных шагах, которые нужно выполнить с начала процесса построения SOC.

On-premise или out-source

Первый, пусть и тривиальный, но важный шаг – это найти, какой SOC будет в вашей организации: так, именуемый on-premise (построенный внутри организации), out-source (на самом деле пасмурный, который находится за границами организации), либо гибридный (когда зависимо от потребностей компания сформировывает свою неповторимую модель SOC, в которой часть ролей и часть функционала берет на себя партнер-интегратор – по модели подписки MDRS, а часть реализуется своими силами и средствами).

Обычно свои центры наблюдения строят организации, обладающие большими ИТ- и ИБ-ресурсами, сильными компетенциями и по ряду обстоятельств не готовые отдавать этот вид работ наружным провайдерам (к примеру, в случае наличия ряда наружных регуляторных ограничений). Аутсорсинг услуг SOC выбирают компании, которым необходим итог здесь и сейчас и у каких нет необходимости оставлять данный пласт работ внутри собственного периметра. Гибридная модель позволяет очень прибыльно соединять услуги аутсорса с функциями своих подразделений.

За этой моделью – будущее, так как данный формат предполагает наилучшее внедрение ресурсов, денежных и трудовых. Но она же просит и определенного уровня зрелости как со стороны систем ИБ самого заказчика, так и со стороны многофункциональных возможностей интегратора-напарника. Есть разные методики оценки нужного варианта SOC, и их показатели будут очень зависеть от специфичности и задач каждой определенной организации. В этой статье будет рассмотрен SOC on-premise, так как конкретно такая модель более трудна в реализации и обычно вызывает много вопросов у наших заказчиков.

Организационная модель

Последующий шаг – это найти организационную модель центра наблюдения. В отношении внутренних SOC обычно выделяют 4 типа моделей, однако на практике мы нередко сталкиваемся с пятой, можно сказать «гибридной».

Команда безопасности. Отсутствует некоторое структурное отделение по обнаружению либо реагированию на происшествия ИБ. В случае появления происшествия ИБ собираются заблаговременно определенные ресурсы (часто из разных подразделений, в том числе ИТ) для решения, восстановления работоспособности систем, после этого команда прекращает свою работу.

Внутренний распределенный SOC. Неизменный SOC существует как некоторое функциональное отделение, но, в главном, состоит из служащих, организационно находящихся за границами SOC, чья главная работа связана с ИТ либо ИБ, но не непременно связана конкретно с защитой компьютерных сетей.

Внутренний централизованный SOC. Выделенное структурное отделение – неизменная команда профессионалов в области ИТ и ИБ. Обеспечивает непрерывную защиту компьютерных сетей, выполняя задачи на неизменной базе в качестве головного вида собственной работы. Ресурсы и возможности, нужные для каждодневной деятельности этого отделения, выделены в некоторую, в официальном порядке утвержденную структурную единицу, обычно со своим бюджетом.

Координирующий SOC. SOC выступает посредником и держит под контролем сотрудничество между несколькими подчиненными ему SOC, обычно работает в больших компаниях с территориально распределенными сетями и филиалами. У организующего SOC чаще всего нет всей полноты картины вплоть до конечного устройства, а возможности в отношении покупателей услуг – ограничены. Однако при всем этом организующий SOC может давать услуги по изучению и расследованию происшествий по требованию подчиненных ему SOC.

Гибридная модель – постоянно располагается в одном из закономерных промежутков между этими 4-мя моделями.

Независимо от размеров и особенностей организации наша команда готова посодействовать с определением и всеохватывающим формированием организационной модели SOC: от коллективного сотворения и проработки многофункциональных матриц RASCI, должностных инструкций либо карточек ролей и возможностей до сотворения соответственных порядков и положений.

Основные задачи SOC

После того как выбрана организационная модель, нужно найти главные задачи SOC. Снова же зависимо от размеров и особенностей организации, задач сотворения центра наблюдения, задачи, которые он должен решать, будут очень различаться, в особенности с учетом разных стадий зрелости компаний.

Время от времени предпосылкой сотворения SOC являются регуляторные требования, при подобном положении и задачи SOC могут просто покрывать определенный набор мер, которые требуются регулятором. Кому-то, с учетом специфичности бизнеса либо организации в общем, этого будет довольно, и это приемлемо.

Остальные компании (обычно это касается уполномоченных лиц ИТ-зависимых отраслей), удачно пройдя этапы целеполагания и определения предпосылок к созданию своего SOC, не желают ограничиваться реализацией регуляторных условий и развивают SOC, повышая зрелость как команды, так и всех применяемых в SOC действий и технологий.

Определяем полномочия

4-й шаг – создать возможности. Они определяют степень свободы в действиях SOC по отношению к защищаемым объектам информационных инфраструктурных объектов – т. е. надобность согласования предлагаемых решений и действий с иными отделениями. Не вдаваясь в детали, можно выделить три главных уровня возможностей SOC, все из них гласит само за себя: Нет возможностей (к примеру, любые решения SOC, либо ИБ в общем, заранее согласовывает ИТ как главенствующая организационная единица); Разделяемые полномочия (по части заблаговременно определенных и согласованных операций и процедур для определенного списка объектов информационной инфраструктурных объектов SOC вправе делать деяния по реагированию либо внесению изменений без каких-то согласований); Полные полномочия (неважно, какая операция либо процедура в отношении хоть какого объекта информационных инфраструктурных объектов, которую нужно выполнить на основании итогов деятельности SOC, производится без промедлений и согласований).

Необходимо подчеркнуть, что возможности SOC никогда не являются и не должны являться безусловными, даже если SOC имеет «полный авторитет» в рамках какой-нибудь сферы собственной работы. Официальные возможности SOC следует применять до определенной границы, после которой SOC должен применять, быстрее, воздействие, чем требования, и непременно прислушиваться к обладателям защищаемых информсистем и data custodian.

На практике же мы нередко смотрим гибридные типы возможностей SOC, которые даже в рамках 1-го центра наблюдения различаются зависимо от определенных бизнес-действий, информсистем либо территориальных подразделений.

Услуги SOC

Последующий шаг – это определение услуг, которые будет оказывать SOC. В качестве примера можно взять методологию MITRE, где все услуги SOC собраны в один большой перечень. Но подчеркнем, что их настолько большое количество, что ни один SOC не сумеет воплотить весь представленный MITRE перечень услуг полностью.

Управление SOC отвечает за выбор услуг в целях выполнения, которые идеальнее всего соответствуют потребностям организации с учетом ее задач, корпоративных и регуляторных ограничений, существующих ресурсов и задач. И конкретно в данном процессе наша команда с удо-

вольствием готова будет посодействовать, также оценив показатели, приобретенные на прошлых шагах, мы сможем вместе с клиентом подобрать и найти список услуг, нужный конкретно его SOC.

Оценка рисков

Без проведения оценки рисков в том либо ином виде, с той либо другой степенью детализации и эффективности приступать к реализации SOC неблагоразумно. Кроме того, что об этом говорят главные отраслевые эталоны и что этого требуют главные отраслевые регуляторы, чрезвычайно принципиально держать в голове, что, лишь основываясь на неизменном и цикличном процессе оценки и изучения рисков, можно получать и актуализировать неоценимые знания о подконтрольном комплексе инфраструктурных объектов, животрепещущих угрозах и, что важно, о приемлемой цене используемых ответных мер, данные по которым недостаточно оценить, очень трудно.

Владея даже частью всех этих познаний, можно достигнуть критически принципиального для SOC состояния – состояния так называемой ситуационной информированности. Это познания о собственном информационном комплексе инфраструктурных объектов (сети), осознание более важных и ценных её частей, особенностях их сотрудничества и преследуемых целях.

Определившись с перечисленными шагами, которые нужно сделать с начала построения центра наблюдения, также достигнув утопии «SOC» либо состояния ситуационной информированности, заказчик сумеет прийти к наилучшему пониманию мотивированной структуры грядущего SOC. Это сделает конечную цель более точной, а значит, и более осуществимой.

Заключение

Трудность опции SOC – это больше вопрос интеграции, чем реализации некоторых модулей. Новые эталоны должны обеспечивать помощь в сокращении разрывов между теоретическими подходами, проприетарными реализациями и автономными системами. При этом вторжения очевидно имеют место, и потому существует надобность для систем оперативного контроля сейчас. Опыт указывает, что нужен рациональный подход, чтобы ввести профессиональный SOC, который может обеспечить надежные показатели.

СПИСОК ЛИТЕРАТУРЫ

1. SOC «с нуля». С чего начать? [Электронный ресурс]: (https://www.angaratech.ru/press-center/novosti/soc-s-nulya-s-chego-nachat-_1252/).
2. Remote Network Monitoring Management Information Base – IETF RFC 1757 – S. Waldbusser – Carnegie Mellon University.
3. Security Operation Center Concepts & Implementation Renaud Bidou [Электронный ресурс на статью]: (https://www.researchgate.net/profile/Renaud-Bidou/publication/228587242_Security_Operation_Center_Concepts_Implementation/links/0f3175318a296d7219000000/Security-Operation-Center-Concepts-Implementation.pdf).
4. Intrusion detection using autonomous agents – Eugene H. Spafford, Diego Zamboni – Computer Networks 34 (2000) 547-570.

SOC құрылысының негіздері

[1]***ҚОБЛАНОВ Нұрбек Бахытұлы,*** *магистрант, n_koblanov@kbtu.kz,*

[1]***СУЛИЕВ Расим Ниязович,*** *PhD, қауымдастырылған профессор, декан, r.suliev@kbtu.kz,*

[1]*Қазақстан-Британ техникалық университеті, Қазақстан, 050000, Алматы, Төле би көш., 59,*

**автор-корреспондент.*

Аңдатпа. *Бүгінгі таңда Security Operation Center (SOC) құру мәселелеріне іс жүзінде отандық экономиканың: сақтандыру компаниялары мен банктерден бастап ірі өнеркәсіптік кәсіпорындарға дейінгі барлық өкілдері қызығушылық танытуда. Мұндай қызығушылық, ең алдымен, үнемі жетілдіріліп отыратын шабуылдардан және оларға қарсы тұрудың заманауи құралына деген қажеттіліктен туындайды. Шынында да, SOC кез-келген ұйымның ақпараттық қауіпсіздік бөлімшесінің негізгі компоненттерінің бірі болып табылады. Бірінші кезекте ол инциденттерге мониторинг жүргізуге, анықтауға және жедел әрекет етуге, соның салдарынан қандай да бір инцидент әкелуі мүмкін залал мен қаржылық шығындарды қысқартуға бағытталған. Қысқа мерзімде нақты нәтижелерге қол жеткізу үшін SOC құруды неден бастау керек? Мақаланың мақсаты – SOC құрастыру кезінде өз тәжірибеміздің алынған ұсыныстарды беру.*

Кілт сөздер: *SOC, on-premise, out-source, АТ, АҚ, тәуекелдерді бағалау.*

SOC Building Basics

[1]***KOBLANOV Nurbek,*** *master student, n_koblanov@kbtu.kz,*
[1]***SULIEV Rasim,*** *PhD, Associate Professor, Dean, r.suliev@kbtu.kz,*
[1]*Kazakh-British Technical University, Kazakhstan, 050000, Almaty, Tole bi str., 59,*

**corresponding author.*

Abstract. *Today, practically all representatives of the domestic economy are interested in building a Security Operation Center (SOC): from insurance companies and banks to large industrial enterprises. This interest is primarily caused by the constantly improving attacks and the need for a modern tool to counter them. Indeed, the SOC is one of the key components of the information security department of any organization. First of all, it is aimed at monitoring, detecting and promptly responding to incidents, and, as a consequence, at reducing damage and financial losses to which this or that incident can lead. How to prioritize, where to start building a SOC to achieve concrete results in a short timeframe? The purpose of the article is to give recommendations obtained from our own experience when building a SOC.*

Keywords: *SOC, on-premise, out-source, IT, information security, risk assessment.*

REFERENCES

1. SOC «s nulya». S chego nachat'? [Elektronnyj resurs]: (https://www.angaratech.ru/press-center/novosti/soc-s-nulya-s-chego-nachat-_1252/).
2. Remote Network Monitoring Management Information Base – IETF RFC 1757 – S. Waldbusser – Carnegie Mellon University.
3. Security Operation Center Concepts & Implementation Renaud Bidou [Elektronnyj resurs na stat'yu]: (https://www.researchgate.net/profile/Renaud-Bidou/publication/228587242_Security_Operation_Center_Concepts_Implementation/links/0f3175318a296d7219000000/Security-Operation-Center-Concepts-Implementation.pdf).
4. Intrusion detection using autonomous agents – Eugene H. Spafford, Diego Zamboni – Computer Networks 34 (2000) 547-570.