SOC: день за днем

ISSP — одна из немногих компаний в Украине, предоставляющая услуги коммерческого SOC, в том числе и за рубежом. О практике работы SOC, о том, с чем приходится сталкиваться и что интересует клиентов, журналу «СиБ» рассказал директор по коммерческим решениям ISSP Артем Михайлов.

Артем МИХАЙЛОВ,
директор по коммерческим решениям компании ISSP

— Какие инструменты вы используете в своем SOC и для чего?

— Основной сервис SOC — это MDR (Managed Detection & Response). Его задача — выявить инцидент и на него среагировать. По большому счету, для этого хватит и SIEM, если телеметрии поступает достаточно. Но для того, чтобы провести дополнительную разведку и сформировать углубленный контекст вокруг событий, мы используем еще около 15 инструментов, в том числе EDR, SOAR, технологии с открытым исходным кодом, такие как Osquery. Сейчас интегрируем в процессы поисковую систему Elastic Stack. Основная услуга обрастает дополнительными мини-сервисами, которые используются в зависимости от ситуации.

На базе собранных знаний об атаках последних лет была разработана автоматизированная платформа оценки компрометации (Compromise Assessment) — GuardYoo. Суть в том, что берется телеметрия за максимально доступный период и выполняется поиск признаков компрометации в ретроспективе. Compromise Assessment показывает основные вспышки аномалий, которые могли пройти незамеченными. Они либо означают что-то настолько новое, что нужно серьезно менять процессы и настройки в инфраструктуре, либо подтверждают деятельность хакеров. В любом случае это новые средства контроля для SOC, чтобы выявлять эти аномалии уже в перспективе.

Compromise Assessment запускается перед подключением клиента к SOC, чтобы понять, какие средства контроля подходят, а какие нужно дополнительно разработать. Если же клиент уже на SOC-услугах, то все равно по прошествии какого-то времени нужно делать встряску. Мы ведь не находимся внутри инфраструктуры и напрямую на нее не влияем; могли появиться новые приложения, измениться какие-то бизнес-процессы. Compromise Assessment дает эту встряску и генерирует пул новых данных.

— Проводя аудит перед подключением клиента, пользуетесь ли вы какими-то стандартами? Как определить, что аудит проведен корректно и действительно обнаружено что-то новое?

— Безусловно, есть ряд стандартов по ИБ, которыми мы руководствуемся: ISO:27001, COBIT и т.д. Однако подключение к SOC не предполагает обязательный GAP-анализ по этим стандартам. Гораздо более полезным сервисом перед подключением к SOC является как раз Compromise Assessment, который демонстрирует реальные аномалии поведения сервисов и пользователей.

Как убедиться, что аудит прошел эффективно? Здесь все просто: если образцы аномального поведения, которые мы обнаружили, для заказчика новость — это значит, что Compromise Assessment прошел успешно. Обычно 80–90% находок являются для заказчика новыми и примечательными фактами, которые влияют на стратегию и тактику управления ИБ.

— Сколько всего сотрудников работает в SOC ISSP и где они находятся?

— В украинском SOC работают порядка 30 сотрудников. В это число входят как операторы, так и архитекторы, которые привлекаются и для других проектов, лаборатория, отдельные узкие специалисты с ключевыми компетенциями, которые по SLA могут быть привлечены для прояснения ситуации. Выявленные аномалии проверяет первая линия операторов из Украины. Если инцидент подтверждается, привлекаются локальные специалисты, потому что нужно взаимодействовать с клиентом, запрашивать контекст, договариваться о дополнительных исследованиях.

— Есть ли некий «усредненный заказ», и если да, то как он выглядит?

— У нас эмпирическим путем выкристаллизовался набор из 21 средства контроля. Это универсальные вещи, которые могут быть применимы как для банка, так и для энергетической компании, потому что в конечном итоге сеть есть сеть. Если заказчик не знает, с чего начать, а оценка компрометации не проводилась, мы по умолчанию предлагаем этот набор. Также просим хотя бы поверхностно дать нам изучить инфраструктуру, чтобы понимать, какой объем данных будем получать, и учесть это в облачных хранилищах и в лицензионных отчислениях производителям.

— Что собой представляет SLA? Существуют ли какие-то его градации или типовой договор?

— Если кратко, то SLA в нашем понимании предусматривает, с одной стороны, ограничение сервиса (входят ли в список получаемых услуг управление журналами регистрации, оценка уязвимости, анализ дампов памяти, очистка трафика и т.д., либо же просто управление инцидентами, а также какой объем информации мы обязуемся получать), а с другой — ответственность сотрудников SOC (как мы классифицируем инциденты и определяем их приоритеты, как быстро и на какие типы инцидентов мы гарантируем реакцию, максимальное время возможной недоступности SOC-компонентов и т.д.).

— Встречаются ли заказчики, у которых вообще никак не выстроена информационная безопасность и они просят, чтобы SOC взял их защиту целиком на себя?

— Бывают, но это незрелый подход. Пока индустрия управляемых сервисов безопасности все равно подразумевает, что какой-то минимальный набор компетенций и возможностей на стороне клиента должен быть.

Сейчас мы автоматизируем не только мониторинг (Detection), но и блокирование угроз (Response). Это юридически и трудно, и опасно, ведь фактически появляется сторонняя компания, которая влияет на бизнес-процессы у клиента, но в некоторых случаях лучше сначала заблокировать, а потом разбираться. Когда удельная доля Response станет большой, необходимость для заказчика иметь ресурсы для поддержки SOC-процессов уменьшится. Но пока у нас по контрактам со стороны клиента есть обязательство выделить как минимум оператора, который взаимодействует с нашим сотрудником, и менеджера сервиса, который следит за выполнением SLA. Это наши «руки» на стороне заказчика.

Сейчас 70–80% отфильтрованных инцидентов, которые являются элементами атаки, мы отрабатываем совместно с клиентом. Наша задача не в том, чтобы клиент забыл о вопросах безопасности и уехал отдыхать, а чтобы он не занимался мониторингом, фильтрованием и прочей рутиной. Заказчик должен четко понимать, что происходит внутри его организации, что мы выявляем и как реагируем.

— А сколько вообще заказчиков используют услугу Response?

— Не больше 10%. Еще 2–3 года назад, за редким исключением, вообще не было культуры мониторинга каждого отклонения от нормы, даже осознания, что нужно эту норму выстраивать. Сейчас совсем другая ситуация, большинство компаний понимают, что за этим нужно постоянно следить, как за кардиограммой. Блокирование — это уже следующий шаг. Компании, пострадавшие от атак, те, у кого был мониторинг и они все видели, но не смогли отбиться, — вот они хотят и блокирование. А те, которые только пришли к необходимости мониторинга, пока морально не готовы сразу переходить на блокирование, они хотят начать с малого, а потом расширяться по мере возможностей. Тут еще можно отметить сходство с DLP-системами. Никто ведь не внедряет DLP сразу в режиме блокировки, нужен период тестирования, чтобы понять, нет ли там большого количества ложных срабатываний. После обучения и оттачивания различных средств контроля уже и мы, и заказчик готовы переключиться на режим блокировки.

— И каким образом вы реагируете, если в данный момент идет атака, например, шифровальщика?

— Шифрование — это была последняя стадия NotPetya. Наша задача — не дожидаться, когда инфраструктура будет захвачена и вирус начнет шифрование; нужно обнаруживать паттерны зловредного поведения на начальных этапах атаки. Для этого используется и оценка компрометации, и Threat Hunting. Но даже если заказчик просто качественно, согласно утвержденному плану выполняет свою часть обработки жизненного цикла инцидента, который мы обнаружили, описали и предоставили рекомендации (например, изменить какие-то процессы, внедрить дополнительные механизмы), — это уже залог того, что до худшего не дойдет.

Что касается NotPetya, у нас действительно был пример, когда один из SOC-клиентов подключился незадолго до атаки, то есть мы не имели возможности обнаружить аномальное поведение на более ранних стадиях, и у него не было услуги Response, а только Detection. Мы ему сообщили, что видим очень плохую активность и надо срочно ограничить такую-то подсеть, но пока там разбирались, шифрование рабочих станций началось. Для нас это был очень важный триггер, прежде мы верили, что блокировку все-таки должен больше делать клиент на своей стороне.

— Сколько примерно стоят услуги SOC?

— На данный момент к SOC ISSP подключены клиенты очень разного размера, из множества отраслей, с разными наборами услуг. Поэтому индикативную цифру назвать невозможно. Недавно мы анонсировали пакет SOC для малого бизнеса, базовый набор такой услуги стартует от $9800 в год (или $820 в месяц). С другой стороны, среди наших постоянных клиентов есть крупная компания, которая ежегодно тратит свыше $100 тыс. на комплексный набор SOC-услуг.

Важно то, что сейчас услуги SOC могут быть предоставлены как точечно, закрывая определенные слабые места, так и в комплексе.

Беседовал **Василий ТКАЧЕНКО**, **СиБ**