OSINT:
новая профессия или тенденция развития ИБ?

Павел КУЗНЕЦОВ,
директор по стратегическим альянсам и взаимодействию с органами государственной власти, Группа компаний «Гарда»

Разведка по открытым источникам (Open Source Intelligence – OSINT), как и многие иные понятия, пришла в информационную безопасность из практик военного управления. Методология OSINT включает в себя сбор, оценку и анализ открыто доступной (публичной) информации в целях дополнения и обогащения имеющихся данных по конкретному вопросу, ранее собранных иными путями. Помимо информационной безопасности OSINT применяется в деятельности различных государственных (например, оборонных и правоохранительных) структур, журналистов и, на самом деле, любых персоналий и организаций, нуждающихся в сборе информации в рамках аналитической или исследовательской деятельности. Рассмотрим основные аспекты OSINT.

Цели и задачи

Основная задача, решаемая OSINT, – получение и тщательный анализ информации, которая доступна в открытых источниках, но иногда ее сложно найти неподготовленному человеку. Открытые источники могут включать социальные сети, блоги, форумы, новостные сайты, различные базы данных и другие онлайн-ресурсы. Важно отметить, что при использовании OSINT необходимо соблюдать законодательство, по крайней мере, если мы говорим о применении этих средств в «гражданских» целях, в том числе в рамках обеспечения информационной безопасности. Обратите внимание: перечисленные источники относятся, так или иначе, к источникам, функционирующим на базе информационно-телекоммуникационных технологий. Как следствие, специалистов по OSINT иногда пренебрежительно называют «профессиональными пользователями Google», но это определение не совсем справедливо, хотя отчасти и указывает на то, что специалист по OSINT – в первую очередь человек, отлично знающий современные информационно-телекоммуникационные технологии и способный уверенно работать в цифровой среде.

Целеполагание OSINT достаточно разнообразно, единственной общей характеристикой является поиск информации о конкретном объекте или субъекте определенных событий.

Государственные органы могут использовать OSINT для расследования преступлений, обращаясь к сбору информации о подозреваемых, преступных группировках, для поиска пропавших людей, предотвращения террористической активности, аккумуляции информации о потенциальных угрозах, оценки международной и внутриполитической обстановки, замера «социальной температуры» в том или ином регионе. В журналистике OSINT может применяться в рамках проверки фактов, вынесения на публику неявно доступных данных о, например, криминогенной обстановке в регионе, жизнь которого освещает СМИ. В информационной безопасности, применяя OSINT в рамках Threat Intelligence (TI) – проактивного анализа угроз с помощью инструментов OSINT можно собирать информацию о группировках атакующих, связях между отдельными атаками и конкретными группировками, их инструментарии, а в отдельных случаях и получать конкретные данные о готовящихся кибератаках. Мероприятия OSINT также полезны при противодействии или реагировании на утечки информации, обнаружении новых инструментов атакующих и многом другом. Ресурсами для поиска при этом становятся поисковые машины, социальные сети, блог-платформы, онлайн-СМИ, форумы, площадки онлайн-торговли, государственные базы данных, в целом – любые иные источники, доступные в глобальной сети Интернет.

Подноготная

В составе современного Security Operations Center (SOC) OSINT применяется в рамках постоянного процесса TI. SOCи ищут релевантные для контекста защищаемого бизнеса угрозы,

признаки готовящихся атак, использования злоумышленниками ранее неизвестных уязвимостей. В рамках проведения расследований специалисты SOC также могут оказывать поддержку правоохранительным органам, чтобы с помощью OSINT установить конкретную личность, стоявшую за произошедшим в защищаемой компании инцидентом информационной безопасности.

Процесс сбора и анализа информации в рамках OSINT, как правило, включает несколько шагов. Сначала необходимо определить цели и требования к информации. Затем исследователь должен выбрать подходящие источники: поисковые системы, социальные сети или специализированные базы данных; рассмотреть необходимость поиска в более сложных источниках, например, в «теневом интернете» (DarkNet). После этого следует провести оценку достоверности источников, чтобы впоследствии выделить наиболее полезные и релевантные данные. Наконец, полученные результаты должны быть организованы и представлены в удобном формате, поэтому о форме отчетности задумываться стоит уже при постановке задачи.

Получить ответ на атомарный вопрос типа «упоминается ли защищаемая компания где-то в сообществах злоумышленников», разумеется, гораздо проще, чем построить некий прогноз, поэтому и спектр инструментов для решения этой задачи может быть сокращен до необходимого и достаточного перечня. Более широкая постановка задачи, к примеру, поиск источника утечки данных или оценка ущерба от утечки (соответственно, требующая нахождения непосредственно утекшего контента), влечет за собой расширение набора требуемых инструментов и увеличение сроков реализации.

Методы и средства OSINT включают как минимум:

- мониторинг новостных и прочих информационных порталов;
- мониторинг социальных сетей, форумов, включая площадки DarkNet;
- использование поисковых движков общего – Google, Yandex – и специализированного – Shodan, FOFA – назначения;
- использование специализированного ПО для сбора и анализа информации, такого как «Гарда Аналитика»;
- анализ открытой финансовой, юридической, банковской, бухгалтерской и любой иной публикующейся отчетности, которая может содержать необходимые данные;
- использование геолокационных сервисов и др.

Существует проект OSINT Framework, объединяющий большой набор ссылок на инструменты OSINT, классифицированные по типу искомой информации.

Нюансы

Помимо преимуществ OSINT имеет ограничения. Например, информация из открытых источников может быть не вполне точной, а чаще всего элементарно недостаточной для квалифицированных выводов по поставленным перед специалистом вопросам. В таком случае необходимо проведение комплексного анализа с использованием данных, полученных другими методами (например, об угрозах от коммерческих провайдеров Threat Intelligence). Кроме того, существует риск «перегрузки» избыточной информацией, когда исследователь сталкивается с большим объемом данных, которые трудно обработать и проанализировать, либо «мусорных» («белый шум»). В некоторых случаях доступ к определенным открытым источникам может быть ограничен или запрещен. Упрощенный пример – переход какого-либо онлайн-СМИ на модель работы по подписке.

В заключение, отвечая на заглавный вопрос, можно сказать, что OSINT – это неотъемлемая часть работы с информацией в современном обществе. Методы и средства OSINT находят применение в различных областях, включая государственные структуры, конкурентную разведку, информационную безопасность и журналистику. В нормативно-правовом пространстве сфера OSINT практически не регулируется, если не считать таковым регулированием, к примеру, закон «О СМИ». При этом, в силу доступности базового набора таких методов любому человеку, они применимы и в повседневной жизни, служа той же цели – более эффективному анализу перед принятием верных решений. Например, оценивая надёжность продавца на площадке интернет-торговли C2C, вы тоже занимаетесь, в некотором роде, OSINT. Поэтому назвать OSINT новой профессией было бы преувеличением. Скорее, это набор навыков, методов и средств, которые очерчивают некоторую дополнительную специализацию представителей той или иной профессии, а отчасти полезных и любому частному лицу, ведь предупреждён об опасности – значит, вооружён для защиты от неё. ■

> OSINT – это неотъемлемая часть работы с информацией в современном обществе.