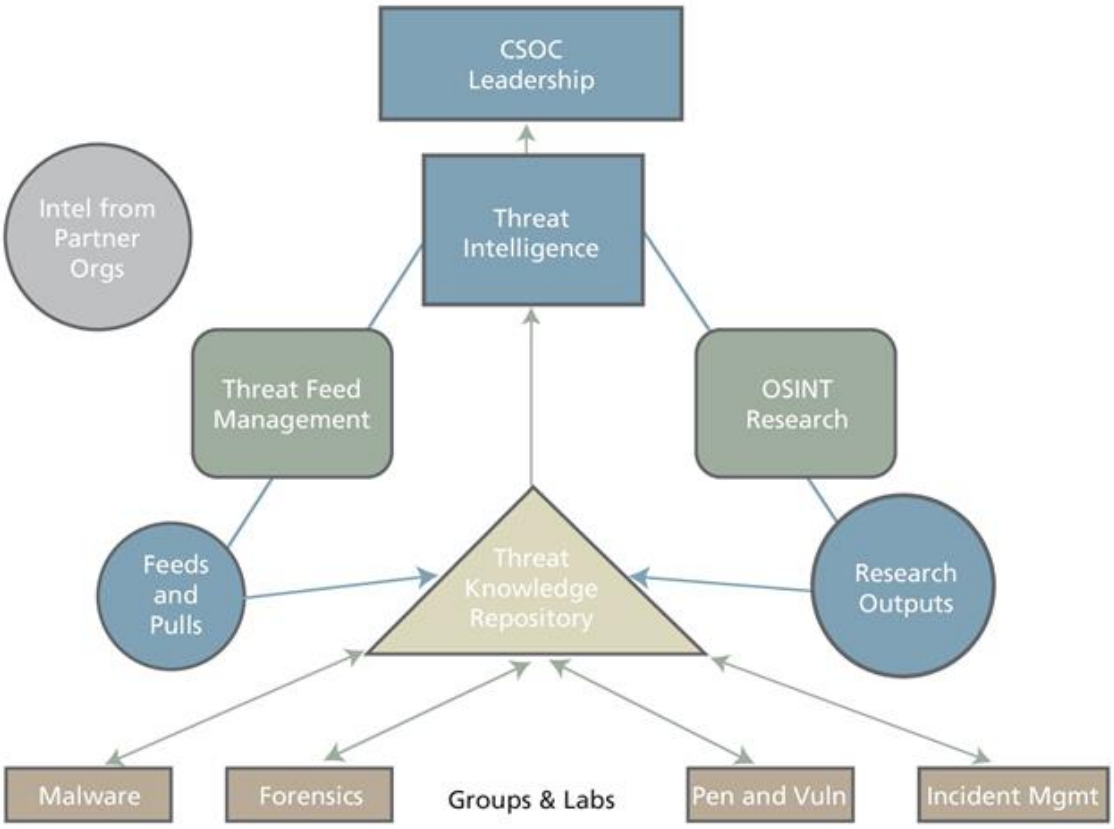
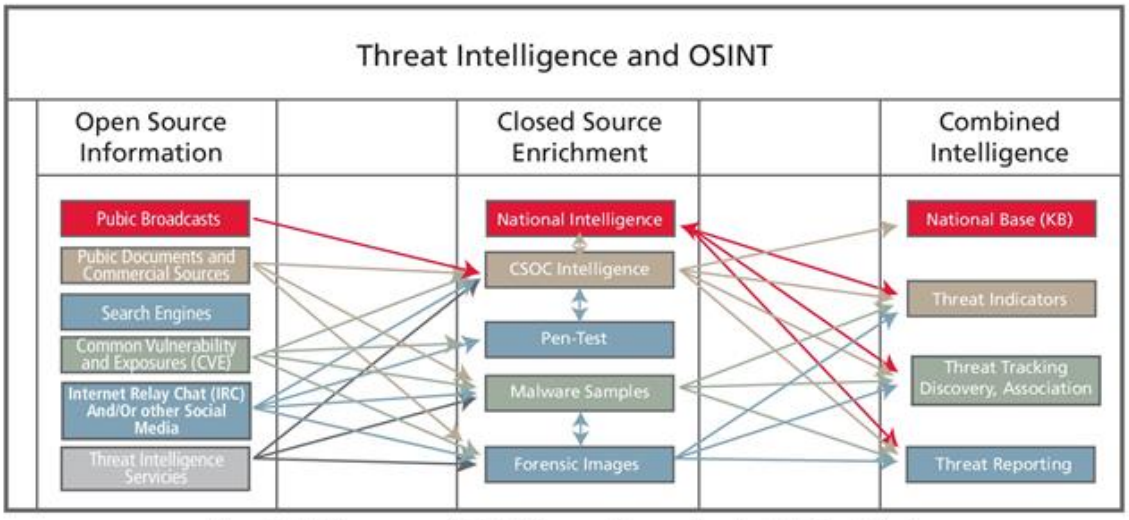


Threat Intelligence Management Model



Threat Intelligence and OSINT Sources Processing for Mission Effect

БИЗНЕС-МОДЕЛЬ OSINT

Полученная система киберразведки предоставит нам реальные данные о том, какие угрозы, уязвимости и тактики используются в мире, какие инциденты и маркеры атак есть в нашей сети и с какими угрозами борются наши коллеги по отрасли. В результате на основе этих данных мы получим ответ на вопрос, когда и какой угрозой нужно заниматься.

Цикл управления угрозами

В 2012 г. в книге «Управление риском и информационной безопасностью: защитить, чтобы сделать возможным» вице-президент и директор по безопасности и конфиденциальной информации корпорации Intel Малкольм Харкинс описал оригинальную модель жизненного цикла угроз (созданную по аналогии с моделью жизненного цикла продуктов Intel). Созданная им модель соединяет в единое целое информацию о развитии угроз, структурированный подход к оценке своевременности разворачивания мер безопасности и ориентацию на мониторинг внешних источников. На её развитие повлиял карьерный путь Малкольма, помимо прочего включавший должности руководителя подразделения конкурентной разведки и ИТ-бенчмаркинга, а также финансового менеджера глобальной ИТ-службы Intel.

Рис. 1. Основные уровни OSINT

Деятельность OSINT (рис.1) условно можно разделить на 3 уровня, каждый из которых обладает собственным содержанием по широте спектра исследуемых проблем, их информационному охвату и глубине временной перспективы изучения:

Стратегический уровень. Призван обеспечить возможности достижения компанией тех долгосрочных стратегических целей бизнеса, которые компания (или отдельный предприниматель) заранее наметила для воплощения в будущем.

Оперативный уровень. Является – специальным видом расследований, как правило, это расследование либо уже прошедших, либо текущих событий/обстоятельств/фактов/и т.п. Непосредственными объектами изучения оперативного уровня исследований выступают внезапные и неожиданные события, которые уже реализовались и оказали свое негативное воздействие на бизнес и деятельность компании.

Тактический уровень. Изучает риски и возможности рыночного характера, касающиеся текущего бизнеса компании. Исследования этого уровня призваны обеспечивать в информационно-аналитическом плане – конкурентоспособность и выживаемость компании в условиях реального времени, т.е. непосредственно в процессе повседневной деятельности компании.

За основу возьмем *модель Харкинса*. Модель Харкинса включает пять фаз развития угрозы: теоретические исследования; экспериментальные исследования;

- доказательство концепции (proof of concept — PoC);
- эксплуатация уязвимостей в продуктах марочной категоиии (багов, недокументированных возможностей и т.п.);
- анализ на основе индикатора компрометации (IOC);
- коммодитизация уязвимости (наличие уязвимостей в ПО производителей крупного масштаба - *commodity*);
- Реализация APT-угроз.

От первой фазы к пятой угроза из высказанной на исследовательской конференции идеи превращается в дешевый общедоступный инструмент атаки на корпоративные инфраструктуры.

доказательство концепции (proof of concept — PoC). Доказательство концепции или доказательство принципа - это реализация определенного метода или идеи чтобы продемонстрировать его осуществимость/целесообразность, или демонстрация как таковая, цель которой заключается в проверки что эта концепция или теория имеет потенциал для дальнейшего использования

В компьютерной ***среде индикатор компрометации (IOC)*** – это активность и/или вредоносный объект, обнаруженный в сети или на конечной точке. Мы можем идентифицировать эти индикаторы и, таким образом, сможем улучшить наши возможности по обнаружению будущих атак.

APT (целевая кибератака) — противник, обладающий современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения. Эти цели обычно включают установление и расширение своего присутствия внутри информационно-технологической инфраструктуры целевой организации для осуществления намерений извлечения информации, создания помех критическим аспектам выполняемой задачи, программы или службы; либо для того, чтобы занять позицию, позволяющую осуществить эти намерения в будущем. APT, как «развитая устойчивая угроза»: добивается своих целей неоднократно в течение длительного времени; адаптируется к усилиям защищающихся оказать угрозе сопротивление; имеет установку сохранить уровень проникновения в целевой инфраструктуре, требуемый для осуществления намерений.

Мы адаптировали модель Харкинса, создав более универсальную, полную и понятную для многих отраслей модель интегрированного мониторинга угроз. Естественно, что модель эта в большей мере рассчитана на выявление развития ландшафта угрозы массовых атак, тактик и инструментов киберпреступности. Она основана на оценке наших гипотез об актуальности того или иного типа угроз по совокупности косвенных признаков.

Этап развития угрозы «Эмбрион»

Гипотеза: существует вероятность новой угрозы или нового типа атаки, реализовать которую очень сложно по любым меркам.

Возможный нарушитель: спецслужбы или кибервойска иностранных государств.

Внешние признаки: угроза обсуждается на конференции, но пока нет её практической реализации.

Внутренние признаки: организация имеет потенциально уязвимые информационные активы (системы, подрядчиков и т. п.).

Признаки у конкурентов: конкуренты обсуждают угрозу.

Этап развития угрозы «Младенец»

Гипотеза: существует вероятность новой угрозы — нового типа атаки или эксплуатации, реализация которой сложна по любым меркам.

Возможный нарушитель: дополнительно кибернаемники (целевые атаки).

Внешние признаки: продемонстрировано подтверждение, но всех деталей и инструментов для атаки нет в общем доступе.

Внутренние признаки: организация имеет потенциально уязвимые информационные активы, доступные на периметре (сетевой периметр, рабочие станции, подключения подрядчиков, BYOD) либо бизнес-критичные (содержащие интеллектуальную собственность, обрабатывающие и хранящие клиентские данные, внешнюю финансовую отчетность и т. п.).

Признаки у конкурентов: конкуренты начали оценивать влияние возможной атаки на бизнес.

Этап развития угрозы «Ребенок»

Гипотеза: существует возможность новой угрозы — нового типа атаки или эксплуатации, реализация которой имеет среднюю степень сложности.

Возможный нарушитель: дополнительно организованная киберпреступность.

Внешние признаки:

- PoC в общем доступе;
- сообщения о реализации угрозы.

Внутренние признаки:

- организация имеет потенциально уязвимые информационные активы;
- отсутствие исправлений от производителя либо невозможность их установки;
- срабатывание характерных для угрозы показателей компрометации (IoC) — взаимодействие с внешними ресурсами, yara-правил (описывают признаки наличия malware), созданных на основании PoC;
- срабатывание антиAPT-решений на поздних стадиях атаки.

Признаки у конкурентов: конкуренты начали прорабатывать проектные идеи противодействия угрозе.

Этап развития угрозы «Подросток»

Гипотеза: существует возможность новой угрозы — нового типа атаки или эксплуатации, реализация которой имеет низкую степень сложности.

Возможный нарушитель: дополнительно массовая киберпреступность.

Внешние признаки:

- в общем доступе обнаружены эксплойты;
- сообщения о реализации угрозы.

Внутренние признаки:

- организация имеет уязвимые информационные активы;
- отсутствие исправлений от производителя либо невозможность их установки;

- срабатывание характерных для угрозы IoC, антивирусов, IDS (Intrusion Detection System);
- срабатывание антиAPT-решений на поздних стадиях атаки.

Признаки у конкурентов: конкуренты начали реализовывать проекты по противодействию угрозе.

Этап развития угрозы «Взрослый»

Гипотеза: ландшафт киберугроз пополнился еще одной угрозой, тактики и уязвимости активно используются в атаках на организации.

Возможный нарушитель: дополнительно хактивисты и хулиганы.

Внешние признаки: эксплойты и методы атаки широкодоступны и дешевы, сообщения в прессе, жалобы клиентов.

Внутренние признаки:

- организация имеет уязвимые информационные активы;
- срабатывание характерных для угрозы IoC, антивирусов, IDS;
- срабатывание антиAPT-решений на поздних стадиях атаки.

Признаки у конкурентов: конкуренты завершили реализацию проектов по противодействию угрозе.

Внедрение модели

Коммерческим компаниям, работающим на конкурентных рынках и стремящимся ограничить корпоративную ответственность, обеспечить непрерывность бизнес-процессов и защитить интеллектуальную собственность, разумно начинать проработку планов защиты от угрозы уже на стадии «Ребенок». Таким образом компании смогут предвосхитить полноценную атаку на свои сети, не неся при этом бремя затрат на этапах «Младенец» или «Эмбрион».

Вместе с тем детальная для предприятий меньших размеров пятистадийная модель может нуждаться в существенном упрощении, ведь ее основы заложила глобальная компания Intel. Однако меньше трех стадий (классический светофор) использовать нерационально, так как будет некогда провести банальное своевременное планирование и бюджетирование проектов.

Можно начать с анализа политики ИБ (подход top-down — «сверху вниз»), вычленив угрозы, которые организация уже считает актуальными (для простоты подразумеваем, что политика содержит модель угроз/архитектуру ИБ прямо или опосредованно, через перечисление ключевых мер снижения рисков информационной безопасности).

Параллельно стоит развернуть IDS и посмотреть, что видно в сети (даже на правилах детектирования по умолчанию), — применим подход bottom-up («снизу вверх»).

Комбинация подходов «сверху вниз» и «снизу вверх» создает подход down-up " вниз и вверх «. Такой подход не только обеспечивает больший обзор угроз, но и повышает авторитет службы ИБ в бизнесе, который обычно использует именно down-up для бизнес-планирования, управления продуктами и бюджетирования. Вообще, применяя используемые бизнесом управленческие практики, служба ИБ позиционирует себя как прагматичное бизнес-подразделение, а не как «очередные гики-айтишники» или «витающие в облаках консультанты».

Сформировав перечень угроз, можно определить, на каком этапе развития угроза находится. К примеру, мобильные угрозы (mobile threats) за последние несколько лет выросли до этапа «Взрослый». Об этом свидетельствуют как статистика вирусов и нашумевшие уязвимости в Android, так и статистика аналитических агентств по намерениям организаций инвестировать защиту мобильных технологий (IT Security Budget Spending Priorities).

Для крупных и глобальных организаций могут быть выделены десятки и даже сотни угроз, для малого бизнеса стоит ограничиться тремя-пятью, возможно до десяти. Слишком большое количество управляемых угроз превратит киберразведку из процесса поддержки принятия решений в очередную «работу в стол». Организация должна быть способна предпринимать действия по итогам мониторинга.

Источники внешних признаков

Внешние признаки можно собрать из трех категорий источников:

- открытая информация (Open Sources, OSINT Sources);
- бесплатные сервисы ИБ-компаний;
- платные сервисы ИБ-компаний.

Открытая информация может быть собрана как в онлайн-, так и в офлайн-источниках:

- специализированные порталы;
- тематические конференции;
- онлайн-СМИ и печатные издания;
- новостные ленты киберкоманд быстрого реагирования;
- базы уязвимостей;
- аналитические отчеты ИБ-компаний;
- хакерские форумы.

Ясно, что организовать полноценный мониторинг внешних источников можно только в очень большой организации, например входящей в ТОП-20 по выручке в стране. Однако кроме очевидной приоритизации (читаем только один отчет-лидер по сетевой безопасности, только один — по безопасности

конечных точек и т. п.) существуют как минимум три стратегии организации мониторинга:

- самостоятельный мониторинг внешних источников;
- потребление внешнего мониторинга;
- смешанная стратегия.

На российском рынке присутствует целый ряд компаний — лидеров мирового рынка кибербразведки: Dell (SecureWorks), CheckPoint, FireEye (iSIGHT Partners), IBM (X-Force Lab), RSA, Symantec. Есть и локальные игроки, в частности, о своем выходе в этот сегмент заявили «Лаборатория Касперского» и Group-IB (отмеченная в Market Guide агентства Gartner наравне с глобальными игроками, но заточенная под банковскую отрасль и угрозы для банковского рынка).

Продукты кибербразведывательных компаний делятся на три уровня — стратегический, тактический и операционный.

Стратегический уровень состоит из четырех основных продуктов:

- отчеты о региональных ландшафтах киберугроз;
- отчеты об угрозах, адресованных конкретным индустриям (например, gaming);
- годовые отчеты об угрозах и форкасты на следующий год;
- отчеты по специфичным угрозам для конкретного заказчика (обычно компании из Fortune 500 со значительной зависимостью бизнеса от ИТ).

Тактический уровень состоит из двух основных продуктов:

- отчеты Situational Awareness о текущей ситуации, например, во время массовых атак на российские банки и сайты государственных организаций;

- отчеты о значимых группировках киберпреступников, уязвимостях и вредоносном коде, в том числе рекомендации по выявлению угроз и закрытию уязвимостей.

Операционный уровень состоит из подписок (feeds), обычно в машиночитаемом виде, содержащих потенциальные индикаторы атак — такие, как IP-адреса атакующих, хэш-суммы вредоносного ПО, выходные ноды TOR, DNS-имена управляющих центров ботнетов и др. Теоретически подписки позволяют повысить детектирующие возможности уже установленных средств защиты, увеличив тем самым отдачу от вложенных в них средств, что особенно актуально в текущих экономических условиях. На практике автор использовал подписки от производителей SIEM в SIEM-проектах, и они действительно помогали находить ранее неизвестные клиентам проблемы в корпоративных сетях банков из ТОП-50.

Обычно существует некий портал, где клиенты могут ознакомиться с доступными им материалами, оставить запрос на новые или посмотреть технические параметры подключения к машиночитаемым подпискам.

В России существует ряд поставщиков, имеющих достаточно информации об угрозах, чтобы де-факто быть ведущими игроками на рыке кибербразведки. Это «Лаборатория Касперского», Group-IB, Positive Technologies, Solar Security (приведены в алфавитном порядке). Всем им было разослано предложение рассказать о бесплатных сервисах в области кибербразведки.

Уточняющие вопросы и последующее отсутствие комментариев от Positive Technologies и Solar Security показали, что эти компании пока не очень «в теме» кибербразведки, и это логично: подобных сервисов на рынок они не выводили.

«Лаборатория Касперского» не представила комментариев, породив ощущение дежавю: в 2015-м компания указала на своем глобальном сайте

целый ряд новых продуктов и услуг — по противодействию целевым атакам, сервисы киберразведки и т. д., — никак не отразив их на российском сайте.

Group-IB представила ответ, опираясь на определение Gartner, и описала свои бесплатные сервисы. Модель продаж сервисов этой компании напомнила мне модель крупнейших новостных агентств, которые продают актуальные уникальные новости лицам, принимающим решения, задолго до того, как эти новости попадут в свободный доступ.

Источники внутренних признаков

Во многих организациях доступен целый ряд внутренних источников:

- журналы доступа пользователей в Интернет;
- журналы событий сетевого оборудования;
- журналы сетевого трафика (внутреннего и проходящего через периметр);
- журналы событий LDAP-каталога;
- журналы работы сервисов;
- журналы средств защиты — IDS, AV и т. п.;
- собственные правила корреляции (handmade IoC);
- аналитика поведения пользователей;
- программы поощрения исследователей за найденные уязвимости (в том числе занимающихся этим ради славы);
- сообщения пользователей.

Умелое использование всех этих инструментов позволит выявить угрозы, которые уже проникли в периметр сети организации.

Источники признаков у конкурентов

Информация о проектах и мерах ИБ у конкурентов по умолчанию закрыта, но и ее можно почерпнуть в целом ряде источников:

- отчеты аналитических агентств (IT Budget Stats, State of Security и т. п.);
- отчеты консалтинговых фирм, в первую очередь Big4 (Global Security Reports и др.);
- тематические конференции;
- тематические СМИ;
- уведомления о закупках;
- личное общение с коллегами;
- собеседования со специалистами;
- услуги по бенчмаркингу службы ИБ, предоставляемые аналитическими агентствами или консалтинговыми фирмами.

Юридическая защита

Ведение разведывательной деятельности исторически являлось прерогативой государства. В связи с этим кибербразведка без соблюдения определенных правил может иметь негативные как для сотрудника, так и для организации в целом последствия.

Для безопасного ведения кибербразведывательной деятельности рекомендуется сформировать список информации, запрещенной к сбору, и, отслеживая изменения в законодательстве, периодически обновлять его.

В список могут войти:

- информация о военных возможностях в киберпространстве страны, резидентом которой является данная организация;
- персональные данные;

- информация с грифом «Коммерческая тайна», «Государственная тайна» и любая другая защищаемая законодательством страны, резидентом которой является организация.

Приложение 1. Пример списка источников

Информация от ИТ-вендоров

- Adobe Security Notification Service
- Oracle Security Alerts
- Технический центр безопасности Microsoft
- Обновления безопасности Red Hat
- Центр безопасности Cisco
- Центр киберразведки Juniper

Информация от ИБ-вендоров и киберкоманд быстрого реагирования

- Исследовательский центр Digital Security
- Публичная лента уязвимостей iDefense
- Исследовательский центр Positive Technologies
- Центр предотвращения угроз CheckPoint
- Центр безопасности Symantec
- Центр угроз HP Enterprise
- Центр угроз IBM X-Force
- Лаборатория безопасности McAfee
- Исследования интернет-угроз TrendMicro
- Аналитика угроз «Лаборатории Касперского»
- Анализ вирусной активности от DrWeb

- Статистика сервиса анализа угроз ThreatExpert
- ККБР (компьютерная команда быстрого реагирования) США (US-CERT)
- ККБР АСУ ТП США (ICS CERT US-CERT)
- Старейшая ККБР (CERT) Университета Карнеги — Меллона (США)
- FireEye M-Trends
- Блог по безопасности Verizon
- Поиск в Deep-Web
- Hacker Intelligence Initiative от Imperva

Информация от провайдеров сервисов anti-DDoS

- Библиотека знаний Arbor
- Портал безопасности Radware
- Центр знаний Akamai

Базы данных угроз

- Реестр взломов сайтов Zone-H
- Рассылки по безопасности Seclists
- Рассылка по уязвимостям FullDisclosure
- Мониторинг деструктивных вирусов Ransomware, проводимый Abuse.ch.
- База данных вредоносного ПО и ссылок Malc0de
- База данных вредоносного ПО и ссылок MalwareDomainLis

Википедия дает следующее определение. Разведка на основе открытых источников (англ. Open source intelligence) — одна из разведывательных дисциплин в американской разведке. Включает в себя поиск, выбор и сбор информации, полученной из общедоступных источников и её анализ.

OSINT - это акроним Open Source Intelligence (англ. - разведка на основе открытых источников), который вошел в обиход в эпоху Интернета и простоты доступа к данным.

OSINT используется как в частном секторе, так и в военных и разведывательных службах в течении многих лет, подходы и источники информации были отобраны и упорядочены специалистами из Лэнгли (там находится штаб-квартира главной американской разведывательной организации). Ныне OSINT доступен всем при помощи нескольких Интернет утилит или приложений, которые можно установить на свои компьютеры дома. Суть всего процесса OSINT во-первых в том, что обязательным является наличии стороны, для которой исследование будет представлять реальную ценность. Во-вторых - это "Анализ", который является ключевым для проведения оценки информации, полученной из открытых источников.

Сегодня компании используют OSINT называя его, однако, "конкурентной разведкой". Можно получить аналитическую информацию по заданной теме исследуя множество медиа и онлайн источников. Эта информация может быть экстраполирована в значимые сведения о компании, лицах, группах или странах, которые они возглавляют. Большинство таких подходов к сбору информации (harvesting) привязаны к онлайн движкам упреждающего анализа (Silobreaker.com и Basistech), которые якобы могут "предсказать будущие действия", как они утверждают. Однако, базовая идея OSINT - это сбор информации для последующего анализа отчетов об Объекте.

Анализ может также привезти к упреждающему анализу поведения и прогнозу, однако все зависит от целей аналитика.

Анализ данных и погрешность/предвзятость

Перед тем как обозначить инструменты и методы OSINT, следует рассказать о "Анализе". Может так случится, что большая часть усилий будет потрачена на сбор информации, которая скорее сбивает с толку или попросту является "дезинформацией". Необходимо уметь отсеивать факты, комментарии и другую информацию, а затем взять то, что было собрано и тщательно проанализировать на предмет ключевой информации. Необработанная информация должна быть проанализирована и аналитик должен решить что верно, а что нет, а также назначить каждому источнику информации свой вес.

Ключ - не быть предвзятым в своем мышлении при проведении OSINT анализа. Примером может служить принятый за чистую монету репортаж Fox News. Всем известно, что Fox скорее отличается своими выдающимися репортерами, нежели объективностью информации. Однако ключевая информация может оказаться правдой. По крайней мере, чтобы создать полную картину об Объекте, необходимо сравнивать и сопоставлять, каждой собранной информации назначать свой вес. Важно сохранять широкий кругозор, и не позволять своему мышлению зацикливаться и плыть по течению. В противном случае, собранная информация, скорее всего будет не корректной.

OSINT может быть связан как с лицами, так и с организациями. В тоже время, люди на деле могут являться частью движения или группы, что сопоставимо реальной компании, таким образом макро и микроисследования очень связаны. Для подтверждения информации может пригодиться и непосредственное взаимодействие с Объектом. Процесс OSINT живой, и аналитик должен быть готов к такому взаимодействию. Надо следовать подсказкам, задавать вопросы, вести подробные записи, чтобы потом

воспользоваться их содержимым. Ключевым является проверка данных и источников, подобно хорошим детективам и репортерам.

Google

Google Search может предоставить много информации для OSINT. Хотя надо стать адептом "Google Hacking", чтобы использовать все возможности Google, т.е. научиться владеть ключами и запросами, которые позволяют получить более детальные результаты. Написано много книг по этой теме, вот несколько базовых запросов, которые могут быть полезны:

- site:.gov | .mil inurl:/FOUO/ filetype:pdf
- site:.mil | .gov "FOUO" filetype:pdf
- site:.mil | .gov FOUO filetype:pdf
- site:.mil | .gov //SIGINT filetype:pdf
- Типы файлов могут быть различными: .xls .pdf .txt и т.д.

Тот же подход использует пентестер для поиска уязвимостей, доступных документов, позволяющих получить доступ к их системам.
Можно использовать Google Alerts для автоматизированного поиска по ключевым словам. Сервис информирует по почте о результатах при каждом новом обнаружении роботами. Удобно то, результат приходит прямо в руки и нет необходимости осуществлять ручной поиск. Поиск применим не только для строк, но и для целых выражения (например, в случае поиска плагиата).
Google Cache предоставляет архивную информацию активных сайтов, архивы отключенных сайтов доступны на сайтах типа Wayback Machine (http://archive.org/web/), созданный для поиска информации по сайтам, владельцы которых не хотят больше публиковать свою информацию.

Поиск по социальным сетям

Twitter, Facebook, Tumbler и прочие социальные сети - это отличный источник информации, где люди, компании и организации выкладывают множество информации, которую не следовало бы размещать. Представленные ниже сайты собирают подобную информацию с помощью поисковых систем и предлагают ее (иногда в графической форме).

- Silobreaker.com
- recordedfuture.com
- Socialmention.com
- addictomatic.com
- whostalking.com
- SamePoint.com
- newsnow.co.uk

Инструментарий WHOIS

Сервис Whois позволяет быстро получить всю информацию о регистрации домена, например, дату регистрации и возраст домена, или узнать контакты, по которым можно связаться с организацией или человеком, чей домен вас заинтересовал.

Whois также часто используют, чтобы проверить домен на занятость и убедиться, что домен свободен и его можно зарегистрировать.

ROBTEX

Лицо может попробовать скрыть факт владения доменом. Это мера может оказаться запоздалой, так как по информации о домене можно сказать довольно многое. Есть много соответствующих инструментов, они легко находятся Google'ом. Часть из них предоставляет связанную информацию, например Robtex. Robtex хорош тем, что предоставляет информацию о домене, о IP-адресе, на котором находится ресурс, о владельце домена, а также о том, какие еще домены используют это же серверное пространство

InfoSniper

InfoSniper - это поисковик с "геолокацией" для IP адресов и доменов, который может указать где сервер находится физически. Такой поиск становится важным в случае расследований, где важна юрисдикция.

Maltego

Maltego - это метапоисковая система и графическая\релационная утилита для анализа базы данных, которую называют швейцарским ножом для сбора данных и OSINT. С помощью каждодневных обновлений, можно получить множество данных, которые могут быть обработаны вплоть до готового результата.

Maltego и "Реляционное отображение". Отличная фича - это наличие маппинга информации в соответствии с ее весом. Это позволяет смотреть на карту и видеть связи между данными, кто с кем взаимодействует и контактирует, как данные соотносятся между собой. Это то, к чему необходимо привыкнуть и использовать в OSINT.

Paterva "Casefile"

Новый продукт компании Paterva, что-то вроде "Maltego Light", однако есть одно серьезное преимущество. Это цифровая белая доска или "доска убийств" как в фильмах о полиции. Можно прикрепить имена и фотографии, создать "case" файлы.