Threat Intelligence:
фиды, признаки компрометации, реагирование

Алексей ЛУКАЦКИЙ,
бизнес-консультант по безопасности, Cisco Systems

Считается, что 98% всех технологий ИБ реактивны. Это приводит к печальным цифрам – среднее время необнаружения вредоносного кода или деятельности злоумышленников в своей инфраструктуре занимает не менее 200 дней (цифры различаются в зависимости от компании, которая считала этот показатель, – от 188 дней у Trustwave, 200 – у Cisco до 305 – у Symantec и 416 – у HP). Почему так происходит? Почему, несмотря на наличие достаточно большого количества средств защиты, мы не в состоянии положительным образом повлиять на свою защищенность? Ответ прост и кроется в том, что мы являемся заложниками выбранных нами производителей средств защиты, которые не могут знать все и оперативно оснащать этим знанием свои решения. И чем меньше производитель, чем меньше у него ресурсов, чем меньше охват, тем медленнее он реагирует на новые атаки и методы злоумышленников.

Разведывательная информация

Threat Intelligence (TI) – это не киберразведка, как часто переводят данный термин на русский язык. И это не только знания, включая процесс их получения, об угрозах и нарушителях, которые обеспечивают понимание методов, используемых злоумышленниками для нанесения ущерба. Самое важное, что существует в определении, – термин «Intelligence». Его часто ассоциирует с понятием «разведка», хотя на самом деле речь идет об информации, которая используется для принятия решений. Иными словами, Threat Intelligence – это не про доступ к фидам с индикаторами компрометации. Это дисциплина, позволяющая иметь основанные на доказательствах знания, в том числе контекст, механизмы, индикаторы, а также практические рекомендации о существующей или потенциальной угрозе для ИТ-активов компании, которые могут быть использованы для принятия решения относительно реакции на угрозу или опасность.

В рамках выстраивания названного процесса в организации мы оперируем не только и не столько статической информацией об отдельных уязвимостях и угрозах, сколько более динамичной и имеющей практическое значение информацией об источниках угроз, признаках компрометации (объединяющих разрозненные сведения в единое целое), вредоносных доменах и IP-адресах, взаимосвязях и т. п. При этом, получая и анализируя такую информацию, мы должны ответить на три вопроса:

- Мы можем принять решение на этой основе?
- Насколько вероятно, что это произошло?
- Мы можем нивелировать ущерб?

Допустим, в фидах Threat Intelligence получена информация о том, что IP-адрес 8.8.8.8 является плохим. Можем ли мы принять решение по этому поводу? Увы, нет, так как на самом деле это адрес DNS-сервера компании Google (и он прописан у многих в настройках браузерах, ОС или сетевых устройств), который мог по ошибке попасть в фиды. А может быть, вредоносная программа просто использовала этот адрес в качестве проверки доступности Интернета (вспомним WannaCry, который обращался к специальному домену в сети Интернет)? С другой стороны, допустим, мы получили информацию о том, что в сети распространяется вредоносный файл с контрольной суммой (хэшем): dc565146cd4ecf b45873e44aa1ea1bac8cfa8fb08614 0154b429ba7274cda9a2 и управлением из контрольного центра, расположенного в домене slimip[.] accesscam[.]org. Мы можем легко принять решение на основе этой информации путем блокирования такого домена на нашем периметре. Можем проверить по журналам регистрации наших средств защиты, сталкивались ли мы с проявлениями этой угрозы. И можем оперативно заблокировать работу файлов с такой контрольной суммой, взаимодействующих с указанным управляющим сервером.

Мониторинг и расследование

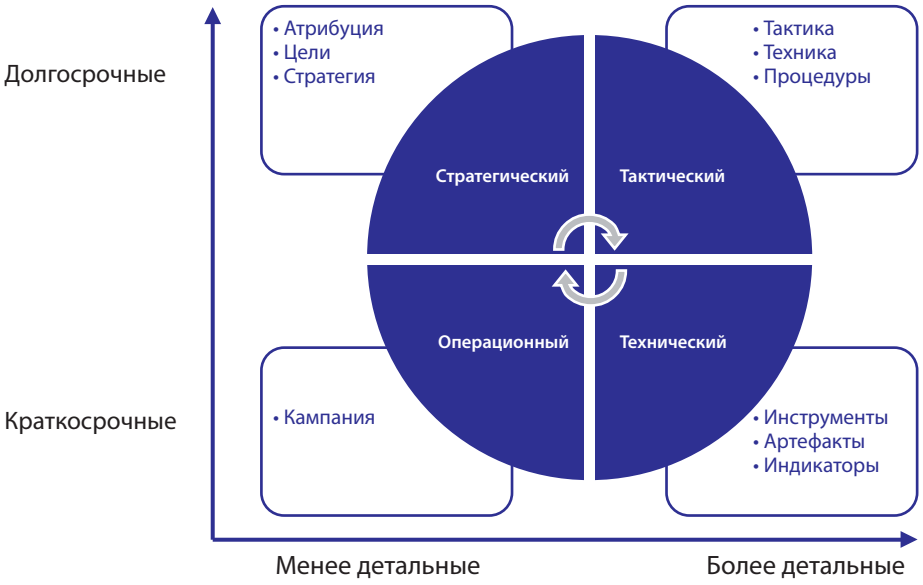
Иными словами, одной из ключевых задач программы Threat Intelligence является повышение качества анализа все более возрастающего объема данных по безопасности, а также помощь в оперативном принятии решений, которое сегодня как никогда важно. Ведь если посмотреть на весь рынок кибербезопасности, то можно увидеть интересную тенденцию: абсолютное большинство производителей перестали декларировать предотвращение угроз, понимая, что это невозможно. Число атак стало настолько велико, а техники и тактики так разнообразны, что гарантировать способность противостоять им всем не решится сегодня никто. Поэтому акцент сместился от предотвращения в сторону обнаружения и реагирования. Фиды Threat Intelligence как нельзя лучше помогают в следующих ключевых процессах.

- Расследование инцидентов. Вы знаете, что один из узлов подхватил вредоносную программу и был скомпрометирован. Но с кем он успел «пообщаться» до того момента, пока его заражение не стало достоянием гласности? Какие файлы появились после заражения? Кому отправлялась электронная почта? Замечены ли в чем-то плохом адреса в Интернете, с которыми взаимодействовал пострадавший? Возможно, они являются частью большой вредоносной инфраструктуры? А может быть, владелец фишингового домена создал еще несколько сотен доменов, с которых в будущем вас могут атаковать? На все эти вопросы также помогает ответить правильно выстроенный процесс Threat Intelligence.
- Поиск угроз (threat hunting). Вы не знаете, скомпрометирована ли ваша инфраструктура, но хотели бы убедиться в том, что внутри нее есть (или нет) следы хакерской активности. Вам надо сформулировать гипотезу и начать поиск следов, подтверждающих либо опровергающих ее. Именно данные Threat Intelligence – адреса сайтов, IP-адреса, хэши файлов, адреса e-mail, URL и т. д. – позволяют найти их в журналах регистрации, именах файлов, почтовом трафике и т. п. и доказать или опровергнуть вашу гипотезу. Иными словами, процесс охоты за угрозами позволяет расширить возможности ваших традиционных средств обнаружения атак.
- Обнаружение вторжений/атак. Вы используете какую-либо из систем обнаружения вторжений, которая по сигнатурам ловит атаки на периметре? Но уверены ли вы в том, что ее производитель знает обо всех угрозах, число которых измеряется десятками миллиардов в сутки? Что если добавить в существующую систему обнаружения поддержку фидов Threat Intelligence, тем самым дав возможность не зависеть от частоты и качества обновления со стороны одного только производителя? Десятки новых источников фидов, подключенных к сенсорам систем обнаружения, и вот мы уже можем видеть в сетевом трафике или журналах регистрации на хостах гораздо больше признаков атак.
- Мониторинг безопасности. Вы построили центр мониторинга безопасности (Security Operations Center – SOC) или просто используете систему класса SIEM и подключили к ним множество источников событий? Теперь ежесекундно к вам поступают тысячи и десятки тысяч событий безопасности? Как разобраться, какие из них реальные, а какие характеризуют ложные срабатывания? Как не отвлекать внимание аналитиков безопасности и отсекать шум? И здесь вновь помогает Threat Intelligence, посредством которой мы обогащаем получаемые события, приоритезируя их, выявляя скрытые взаимозависимости и объединяя в инциденты. К примеру, служба безопасности Cisco ежедневно фиксирует 1,2 трлн (!) событий ИБ (это, к слову, в три раза больше, чем ожидаемое количество звезд в галактике Млечный путь). Но после обработки и применения Threat Intelligence остается всего 22 инцидента, с которыми уже и работают специалисты по кибербезопасности.

> Абсолютное большинство производителей перестали декларировать предотвращение угроз, понимая, что это невозможно.

Но Threat Intelligence – это не только фиды с индикаторами компрометации, которые часто ассоциируются с понятием «кибербразведка». Это всего лишь один из ее «продуктов». Принято выделять четыре уровня данных Threat Intelligence:

- технический. Привычные фиды – небольшие порции данных, которые «скармливаются» (отсюда и слово feed) системам аналитики в области кибербезопасности. Они описывают признаки угроз, с которыми кто-то уже столкнулся, – IP/URL/DNS/e-mail-адреса, имена, контрольные суммы и иные метаданные файлов. Для описания фидов и их передачи различным средствам защиты было разработано немало стандартов. Общепризнанными являются STIX и TAXII, которые используются



российскими регуляторами, ФСБ и Банком России, рассылающими своим подопечным данные об угрозах;

- тактический. Атомарные индикаторы, характеризующие те или иные хакерские инструменты, используются различными техниками злоумышленников, которые позволяют последним достигнуть их тактик – оставаться незамеченными, перехватывать управление, повышать привилегии, подбирать пароли и т. п. Объединенные в техники и тактики эти индикаторы позволяют лучше понять, как могут быть атакованы и скомпрометированы наши ИТ-активы. Стандартом де-факто в описании тактик и техник стала так называемая матрица ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), на базе которой и наш регулятор, ФСТЭК, разрабатывает сейчас методику моделирования угроз и обновляет свой банк данных угроз;
- операционный. Наборы техник и тактик определяют ту или иную вредоносную операцию, совершаемую хакерскими группировками, которые обладают своим почерком. Выстроив процесс Threat Intelligence на этом уровне, мы можем уже делать обоснованные выводы о том, случайно ли нас задела какая-то атака или против нас развернута целая кампания, за которой может стоять государство или просто продвинутая группа киберпреступников;
- стратегический. На этом уровне как раз и определяется, кто стоит за той или иной атакой на нашу организацию, т. е. проводится атрибуция, позволяющая ответить на традиционный вопрос любого начальника «кто виноват?».

> Стандартом де факто в описании тактик и техник стала так называемая матрица ATT&CK.

Зрелая разведка

Перечисленные четыре уровня отражают зрелость процесса Threat Intelligence в организации, а также затрачиваемые на их реализацию энергию и ресурсы. Проще всего оперировать атомарными индикаторами, которые можно получать из множества частных и публичных, коммерческих и государственных, отраслевых и международных источников фидов (например, от Cisco, Microsoft, VirusTotal, SANS, AlienVault, Abuse.ch, Spamhouse, Spamcop и др.). Объединение их в тактики, увязывание с кампаниями и операциями и последующая атрибуция – это уже высший пилотаж, который сегодня доступен далеко не всем компаниями, причем не только в России, но и в мире. Все-таки нехватка специалистов по кибербезопасности сказывается везде, в том числе и в сфере киберразведки.

Сегодня почти все компании, зачастую даже неосознанно, реализуют первый, технический уровень процесса Threat Intelligence, подключая к своим средствам защиты и анализа различные источники фидов, со списком которых можно ознакомиться по адресу https://github.com/hslatman/awesome-threat-intelligence. При их выборе можно опираться на следующие критерии:

- автоматизация;
- интеграция и интероперабельность;
- частота обновлений;
- обогащение метаданными;
- рейтинг сложности;
- покрытие;
- видимость теневого Интернета;
- аккуратность в геолокации;
- количество и спектр источников;
- качество.

Получаемые из различных источников фиды, а среди них есть и российские (например, ГосСОПКА или «ФинЦЕРТ»), обычно загружаются и анализируются в специализированных TI-платформах, которые позволяют собирать индикаторы компрометации из источников, классифицировать их и производить

с ними различные операции, в том числе выгрузку в средства защиты и системы мониторинга (SIEM). К числу таких решений относятся и коммерческие игроки рынка (например, Anomali, ThreatQ или BI.ZONE), и бесплатные инструменты (CRITs, CIF, GOSINT, MANTIS, MISP, MineMeld, Yeti и др.).

При анализе рынка и выбора платформы и провайдера для Threat Intelligence следует обратить внимание на ряд моментов. Прежде всего, крупные производители средств защиты имеют собственные процессы/подразделения Threat Intelligence и, вероятно, у них есть возможность получать такие данные и аналитику в рамках существующих контрактов. Например, Cisco купила в свое время ThreatGRID и Umbrella, а AT&T – компанию AlienVault. Из российских игроков можно назвать «Лабораторию Касперского», Group-IB, BI.ZONE и «Солар-Ростелеком». Также существуют самостоятельные компании, предоставляющие услуги Threat Intelligence всем желающим, например IQRisk, ETPro, ThreatStream. Ну и не стоит сбрасывать со счетов отраслевые и государственные центры обмена информацией Threat Intelligence, в частности ISAC в США или НКЦКИ и «ФинЦЕРТ» в России.

Пять шагов к успеху

Однако если мы не хотим ограничиваться только техническим уровнем Threat Intelligence и перед нами стоит задача выстроить целую программу, то придется реализовать пять шагов, на каждом из которых последовательно ответить на следующие вопросы.

1. Планирование:
   - зачем нам Threat Intelligence?
   - какие у нас требования?
   - кто может атаковать нас (модель нарушителя)?
   - нюансы (геополитика, отрасль, уровень TI…)
   - своя или внешняя платформа Threat Intelligence?
   - выстраиваем свой процесс или отдаем все на аутсорсинг?
2. Сбор данных:
   - что может провайдер TI (источники)?
   - возможности провайдера TI стыкуются с вашими потребностями?
   - кто внутри вас будет общаться с провайдером TI и как?
3. Обработка и анализ:
   - как сырые данные превратятся в TI?
   - платформа для обработки и анализа?
   - кто проводит анализ?
4. Распространение информации об угрозах:
   - кому можно распространять информацию? На каких условиях?
   - какие стандарты используются для распространения?
   - когда распространять информацию?
5. Разбор полетов:
   - какие действия необходимо произвести на основании полученных данных?
   - как взаимодействовать со средствами защиты?

В рамках одной статьи довольно сложно описать все нюансы построения программы Threat Intelligence на предприятии. Подобная программа как никогда важна в сложившейся ситуации для каждой организации, отрасли и даже государства. В условиях, когда количество возможных нарушителей постоянно увеличивается, а спектр возможных атак уже не поддается исчислению, система сбора и анализа информации должна стать неотъемлемой частью эффективной системы ИБ на предприятии. Сегодня есть все возможности, ресурсы и инструменты для построения такой системы, но при ее создании необходимо самое пристальное внимание уделить стандартизации и автоматизации (включая обновления) – без них эффективной системе Threat Intelligence, интегрированной с используемыми в организации средствами ИБ и аналитики, не бывать.

> Программа Threat Intelligence как никогда важна в сложившейся ситуации для каждой организации, отрасли и даже государства.

Вопросы для самопроверки

Ну и, наконец, пара практических советов, с которых можно начать выстраивать процесс Threat Intelligence. Во-первых, ответьте на два вопроса. Первый: «Какие инциденты были самыми популярными у вас за прошедший год?». Программы-вымогатели, фишинг, вредоносное ПО, DDoS? Второй вопрос будет звучать так: «Какие типы нарушителей были самыми популярными». Киберпреступники, инсайдеры или вас атаковали зарубежные государства? Ответив на эти вопросы, вы сможете сфокусироваться на том, для каких типов угроз и нарушителей вам нужны будут данные Threat Intelligence, и выбрать наиболее релевантные для вас источники. Что же касается платформы для сбора и анализа получаемых данных об угрозах, то стоит начать с какого-либо решения с открытыми кодами, например MISP, на котором можно будет, не тратя больших финансовых ресурсов, отработать базовые вещи, связанные с киберразведкой. ■