1 Введение в охоту за угрозами

В этой главе

- ✓ Этапы Cyber Kill Chain.
- ✓ Как охотники выявляют подозрительную активность.
- ✓ Чем охота за угрозами отличается от обнаружения угроз.
- ✓ Как гипотезы помогают выстраивать процесс охоты.
- ✓ Факторы, определяющие успех охоты за угрозами.
- ✓ Основные инструменты охотников.

Глава знакомит с Cyber Kill Chain, содержит обзор современного ландшафта киберугроз и показывает, как охота за угрозами помогает справляться со сложными вызовами для информационной безопасности. Мы обсудим, как мыслит охотник за угрозами, и рассмотрим фундаментальные принципы эффективной программы. Отдельно будут показаны сходства/различия между охотой и выявлением угроз. Завершится глава обзором инструментов, без которых не обойтись специалисту в данной сфере. А начнем мы с обзора ландшафта киберугроз и разберемся, почему охота за ними сегодня так важна.

ОПРЕДЕЛЕНИЕ В этой книге охота за киберугрозами определяется как практика безопасности, опирающаяся на человеческий фактор. Она основана на проактивном подходе к выявлению угроз, которые смогли обойти средства обнаружения, а также тех, что были обнаружены, но отклонены или недооценены человеком.

1.1. Ландшафт киберугроз

На сегодня ландшафт киберугроз сложен, постоянно развивается и отличается большим разнообразием. Действующие злоумышленники — от организованных киберпреступных группировок до структур, поддерживаемых государствами, — совершенствуют существующие методы и инструменты атак, а также создают новые, чтобы преодолевать этапы Cyber Kill Chain.

На рис. 1.1 показана Cyber Kill Chain, разработанная компанией Lockheed Martin (https://mng.bz/KD5X). Она представляет собой набор шагов, которые злоумышленники обычно проходят, чтобы достичь своей цели. Cyber Kill Chain включает семь этапов.

1. *Разведка*. Злоумышленник собирает информацию, чтобы определить потенциальные цели и тактики атаки. Например, он может получать данные из социальных сетей или сканировать публичные приложения на уязвимости.
2. *Вооружение*. Злоумышленник разрабатывает код для эксплуатации уязвимостей или слабых мест, выявленных на этапе разведки. Например, готовит фишинговое письмо, код SQL-инъекции или вредоносное ПО.
3. *Доставка*. Злоумышленник использует каналы доставки для отправки подготовленной вредоносной нагрузки. Например, может разослать вредоносный код по электронной почте.
4. *Эксплуатация*. Злоумышленник выполняет код, подготовленный на этапе вооружения.
5. *Установка*. Злоумышленник обосновывается в системе, создавая канал для доступа к скомпрометированному устройству.
6. *Командование и управление*. Злоумышленник устанавливает канал связи с внешним сервером. Например, может использовать платформу *X* как скрытый канал управления для взаимодействия с зараженными системами.
7. *Выполнение действий*. Злоумышленник выполняет основную задачу атаки. Например, оператор программы-вымогателя может зашифровать файлы на взломанном ресурсе.

Рис. 1.1. Cyber Kill Chain, разработанная компанией Lockheed Martin

В кибербезопасности популярен мем, приписываемый Дмитрию Альперовичу: «Сегодня существует два типа компаний: те, кто знают, что их взломали, и те, которых взломали, но они об этом еще не знают». Охота за угрозами позволяет организациям действовать проактивно — исходить из того, что их уже взломали, и искать подтверждения этому.

1.2. Почему охота за угрозами так важна

Идеального киберпреступления не существует. Злоумышленники оставляют следы и улики на каждом этапе Cyber Kill Chain. Поэтому опытные хакеры ушли от «шумных» взломов, которые сразу поднимают тревогу, к скрытным действиям с минимальным «отсвечиванием», почти не вызывающим срабатываний (а порой и вовсе незаметным) автоматизированных систем обнаружения. Согласно отчету Института SANS, «развитие таких угроз, как бесфайловое вредоносное ПО, программы-вымогатели, эксплойты нулевого дня и сложные типы вредоносного ПО, в сочетании с обходом средств защиты формирует экзистенциальный риск для предприятий» (https://threatpost.com/2021-attacker-dwell-time-trends-and-best-defenses/166116/).

Прогрессирующая изощренность злоумышленников в скрытых операциях и их способность запускать атаки, практически не выявляемые стандартными средствами защиты, требует от организаций подходов, выходящих за рамки обычных средств обнаружения. Изменившееся поведение злоумышленников вынуждает защитников внедрять проактивные методы, в том числе охоту за угрозами, а также использовать продвинутую аналитику на основе статистики и машинного обучения. Охотники могут регулярно проверять возможные сценарии утечки данных через систему доменных имен (DNS), используя статистические методы анализа по объему трафика. Им не нужно дожидаться, пока сетевые средства защиты, такие как системы обнаружения вторжений (IDS), сгенерируют оповещение, и полагаться только на них.

Охотники за угрозами помогают организациям выявлять атаки, не замеченные средствами защиты. Благодаря этому сокращается время присутствия злоумышленников в системе, а устойчивость повышается. *Время присутствия* — это промежуток между первоначальным проникновением в среду (временем первой успешной эксплуатации уязвимости) и моментом, когда организация обнаруживает факт атаки. Помимо сокращения данного периода, охота за угрозами дает и другие преимущества в рамках обеспечения безопасности, среди них:

- выявление недостатков в механизмах предотвращения и обнаружения атак;
- корректировка существующих сценариев мониторинга защищенности;
- выявление новых сценариев мониторинга защищенности;
- обнаружение уязвимостей, которые не были выявлены в ходе оценочных мероприятий;
- выявление ошибок конфигурации в системах и приложениях, которые могут сказаться на безопасности, работе или соблюдении требований.

Чтобы добиться этих эффектов, организации выстраивают отлаженный процесс охоты за угрозами и заранее определяют, что требуется на старте (гипотеза, источники данных, метрики) и каким должен быть итог каждого сеанса (выявленные признаки атаки, зарегистрированные инциденты, рекомендации по мерам). Эта книга поможет вам выстроить эффективную программу охоты за угрозами с опорой на практические примеры и шаблоны.

1.3. Структурирование охоты за угрозами

Охота за угрозами опирается на подход, основанный на гипотезах. *Гипотеза* — это утверждение, согласующееся с имеющимися данными, но еще не подтвержденное и не опровергнутое. Хорошая гипотеза привязана к среде конкретной организации и поддается проверке с учетом доступных данных и инструментов. Такой подход и называют *структурированной* охотой за угрозами.

Напротив, *неструктурированная* охота подразумевает, что охотники анализируют имеющиеся данные на предмет аномалий без заранее сформулированной гипотезы. Охотник может обрабатывать и визуализировать данные в поисках неожиданных изменений в закономерностях — например, аномальных всплесков или провалов сетевого трафика. Такие находки становятся отправной точкой для дальнейшего расследования и помогают выявлять ранее не замеченные угрозы. Эта книга сосредоточена на структурированной охоте, но я не отговариваю вас время от времени исследовать данные и без формальной гипотезы. Пример гипотезы для охоты:

> *злоумышленник получил доступ к одной/нескольким конечным точкам Microsoft Windows. В частности, он пользовался PowerShell — для запуска команд, не предусмотренных политиками безопасности.*

1.3.1. Формулирование гипотезы

Ландшафт киберугроз, характерный для защищаемой вами среды, должен задавать направление формулируемых и проверяемых гипотез. Разные источники сведений об угрозах и их релевантности помогают охотнику понять ситуацию и на основе полученных данных выдвигать гипотезы. Примеры таких источников:

- внутренние и внешние источники данных о киберугрозах;
- результаты моделирования угроз;
- результаты учений красной команды (red team);
- обзоры действующих стандартов и методологий в области угроз;
- анализ прошлых и текущих инцидентов в сфере ИБ.

1.3.2. Проверка гипотезы

Задача охотника за угрозами — проверять гипотезу, используя все доступные ему средства. Стоит начать с краткого перечня действий, которые помогут найти первые свидетельства/индикаторы по гипотезе или наметят последующие направления исследований. Так, поиск подозрительной активности в среде PowerShell может выявить факт компрометации и подтвердить гипотезу, приведенную в начале раздела. Успешное выполнение требуемых шагов может привести к обнаружению следующих признаков компрометации:

- подозрительная закодированная PowerShell-команда;
- подозрительный запуск неподписанных скриптов PowerShell без вывода предупреждений;
- PowerShell-процесс с подозрительными аргументами;
- подозрительный родительский PowerShell-процесс.

Эта книга описывает разные приемы для выявления сценариев угроз, в том числе связанных с активностью в среде PowerShell. Когда вы проводите охоту, возможны три исхода.

- *Гипотеза подтверждена.* Анализ данных, собранных в ходе охоты, подтверждает гипотезу. В этом случае выявляется угроза безопасности.
- *Гипотеза опровергнута.* Анализ данных, собранных в ходе охоты, показывает, что гипотеза неверна. В этом случае угроза безопасности не обнаружена.
- *Неопределенный результат.* Недостаточно информации, чтобы подтвердить или опровергнуть гипотезу. Такое бывает из-за ограниченного охвата, нехватки данных или неподходящих инструментов.

ВНИМАНИЕ! То, что гипотеза не подтвердилась, не означает, что угрозы нет. Это значит лишь, что при имеющихся компетенциях, данных и инструментах охотнику не удалось ее выявить.

1.3.3. Процесс охоты

Охота может занять от часа до недели — все зависит от ряда факторов.

- *Начальные проверки.* Сколько изначальных сценариев нужно отработать, чтобы получить первые зацепки.
- *Данные.* Объем данных, сложность запросов и производительность инструментов. Например, поиск 1 Тбайт данных в «горячем» хранилище (диски с высокой скоростью операций ввода-вывода в секунду, IOPS) будет выполняться заметно быстрее, чем тот же запрос по данным в «холодном» хранилище (низкая скорость IOPS).

- *Сложность угроз*. Сложные атаки, связанные с APT (advanced persistent threat — «продолжительная атака повышенной сложности»), для полноценного расследования могут требовать недель или месяцев. Это не значит, что охота растянется на месяцы; скорее, она просто займет больше времени, чем обычно.
- *Доступ к данным и системам*. Отсутствие оперативного доступа к ним во время охоты затягивает процесс. Например, если охотнику вовремя не предоставляют доступ к результатам, которые получила другая команда, придется ждать, искать более затратные и менее надежные решения — или завершить охоту без определенного результата.

Эта книга сосредоточена на структурированной охоте, когда охотник вместе с другими специалистами по информационной безопасности формулирует и проверяет гипотезу, нацеливаясь на тактики, техники и процедуры (tactics, techniques, procedures, TTP) злоумышленника.

> **ОПРЕДЕЛЕНИЕ** Под структурированной охотой понимается использование четко определенной последовательности шагов для запуска, проектирования, проведения и документирования охоты за угрозами.

Со временем программа охоты становится более отлаженной и эффективной — охотники извлекают уроки из каждого сеанса. Книга содержит практические рекомендации по планированию, построению и операционному управлению программой охоты за угрозами.

1.4. Охота за угрозами или обнаружение угроз

Обнаружение угроз — это преимущественно инструментальная функция, тогда как охота за угрозами опирается на человеческий фактор. В охоте в центре внимания охотник; при обнаружении ключевую роль играют средства и системы. Охота сильно зависит от опыта специалиста: он формулирует гипотезу, ищет свидетельства в больших массивах данных и постоянно переориентирует поиск, переходя от одной зацепки к другой. При этом охота не заменяет технологии обнаружения — она дополняет их.

Под *обнаружением угроз* понимается реактивный подход, когда аналитики SOC (security operations center) реагируют на оповещения, которые сгенерировали инструменты. Специалисты проводят первичную оценку событий (triage) и расследование инцидентов (например, изучают сгенерированные EDR- и SIEM-системами оповещения).

На практике процесс обнаружения выглядит так (рис. 1.2): аналитики SOC обрабатывают поступающие оповещения. Это похоже на фермерство: как фермеры ждут поспевания урожая, так и аналитики SOC ждут, когда «созреют» оповещения на дашборде, чтобы разобрать их и отреагировать.

Охота, напротив, проактивный подход. Охотники берут инициативу на себя: выходят «в поле» и охотятся, опираясь на правильный образ мышления, опыт, ситуационную осведомленность и инструменты. В разделе 1.6 этот процесс описан в общих чертах.

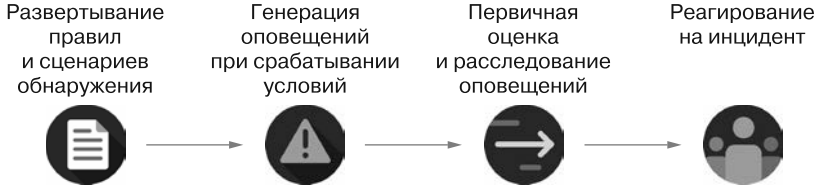

Рис. 1.2. Процесс обнаружения угроз в общих чертах

Обнаружение — ключевая функция SOC. При создании или делегировании функции охоты за угрозами устранение пробелов в мониторинге защищенности должно быть главным приоритетом. Запуск программы охоты нельзя рассматривать как способ «переложить» работу команды мониторинга защищенности на охотников.

Обнаружение и охота осуществляются в связке, обеспечивая более широкий охват ландшафта киберугроз. Эти практики взаимодействуют и частично пересекаются: часто результаты обнаружения угроз становятся вкладом в охоту и наоборот. Например, охотник может выдвинуть гипотезу о массовой компрометации системы, опираясь на подозрительные события, зафиксированные в одной или нескольких конечных точках и замеченные командой мониторинга.

Обе практики — и обнаружение, и охота — опираются на аналитические методы для выявления признаков вредоносной активности. Так, инструменты поведенческой аналитики пользователей задействуют статистические данные и алгоритмы машинного обучения, чтобы выявлять и сообщать об аномальном поведении команде мониторинга. Охотники могут применять аналогичные подходы в своей работе. Хотя они обычно не разрабатывают модели машинного обучения, им важно понимать возможности и ограничения различных аналитических техник.

> **ПРИМЕЧАНИЕ** В главе 2 я расскажу, почему и каким образом охота и обнаружение интегрируются в единый процесс. Я детально разберу процесс интеграции практики охоты с другими функциями безопасности, включая обнаружение, — с анализом этапов подготовки, проведения и коммуникации в рамках общего сценария.

1.5. Квалификация охотника за угрозами

Охотник за угрозами — это специалист ИБ, который проактивно и целенаправленно ищет атаки и угрозы, ускользнувшие от развернутых в сети технологий обнаружения. Успешных охотников отличают любознательность, готовность браться за поставленные задачи и хорошее понимание ландшафта угроз в своей среде.

В работе вы столкнетесь с разнообразными трудностями, такими как недоступность данных, медленные поисковые запросы, некорректный анализ событий, устаревшие технологии, неполный или вовсе отсутствующий доступ к системам. Обсуждайте эти проблемы во время и после охоты (при подведении итогов). Что-то удастся исправить быстро, а что-то затянется или вовсе не получится, особенно если требуются финансовые вложения. Это не должно мешать вам повышать результативность охоты: ищите альтернативные источники данных и систем, оттачивайте используемые приемы.

Охотники — находчивые люди. Наступательный подход дает им преимущество при разработке сценариев охоты и проведении сеансов.

Если в ходе сеанса гипотезу подтвердить не удалось — не расстраивайтесь. Такой исход предсказуем и может объясняться разными причинами, например:

- описанной в гипотезе атаки/угрозы на самом деле нет;
- у охотника мало контекстной информации об инфраструктуре (к примеру, охота проводится в недавно развернутых системах);
- не хватает компетенции для выявления сложных атак в незнакомых технологиях (скажем, вы можете не иметь достаточного опыта в Kubernetes и контейнерах);
- отсутствуют нужные данные для более тщательного исследования;
- применяются неподходящие техники для обнаружения сложных атак (базовые запросы редко помогают против APT).

Никто не ожидает, что охотник знает все. Успешные специалисты регулярно исследуют новое и пробуют новые тактики, техники и процедуры. Ландшафт ИБ динамичен, и большее время на исследование заметно увеличивает шансы обнаружить продвинутые угрозы.

> **ПРИМЕЧАНИЕ** В главе 2 подробнее рассматриваются роли и обязанности охотников, а в главе 13 — как повысить эффективность их действий.

1.6. Процесс охоты за угрозами

Определение процесса помогает охотникам выстраивать, проводить и постоянно улучшать как общую практику, так и отдельные сценарии охоты, повышая со временем вероятность выявления угроз. Это приносит организации дополнительные результаты — например, ведет к обновлению существующих и созданию новых правил обнаружения и данных киберразведки.

На рис. 1.3 показан процесс в общих чертах. Он начинается с формализации гипотезы и попытки ее подтвердить. Если это не удается, ее уточняют (дополняют детали) и повторяют поиск. В случае подтверждения гипотезы стоит говорить о выявлении угрозы. На этом охотник не останавливается: он расширяет охват и ищет

индикаторы в других системах, чтобы понять масштаб и распространение атаки. Далее охотник подключает команду реагирования на инциденты и делится новыми данными, которые помогут командам мониторинга безопасности и кибербразведки.

Рис. 1.3. Процесс охоты за угрозами в общих чертах

Рассмотрим основные этапы охоты за угрозами.

1. *Сформулировать гипотезу*. Определить гипотезу на основе данных из разных источников и процессов: результатов моделирования угроз, тактики, техники, процедуры от внутренних и внешних провайдеров данных кибербразведки, а также поиска тактик и техник в базах знаний (например, MITRE ATT&CK). Команда кибербразведки может, к примеру, отслеживать хакерские группировки вроде APT39 (https://mng.bz/znr1), нацеленные на правительства Западной Европы, внешнеполитические организации и им подобные. Охотник формулирует гипотезы, опираясь на релевантные тактики и техники этой группы.

   Перед переходом к следующему шагу охотник отвечает на такие вопросы.

   - Какие действия ему необходимо предпринять для подтверждения гипотезы?
   - К каким данным ему нужен доступ?
   - Каков объем этих данных?
   - Сколько времени займут поиски и как их оптимизировать (в том числе при помощи специалистов по платформе)?
   - Какими инструментами он будет пользоваться?

2. *Искать подтверждения гипотезы в целевой среде*. Искать признаки, свидетельствующие в пользу гипотезы.

3. *Если гипотеза не подтверждена — доработать и вернуться к началу.* Оптимизировать сценарий охоты: расширить охват, запросить доступ к системным данным, скорректировать поисковые действия или уточнить саму гипотезу.
4. *Если гипотеза подтверждена* — выполнить дальнейшие шаги.
   - *Сменить фокус и расширить охват.* Оценить масштаб инцидента, расширив границы охоты.
   - *Сформулировать (дополнить или создать) правила обнаружения и обновить данные киберразведки.* Рекомендовать новые правила детектирования для мониторинга и обновить материалы киберразведки, передавая индикаторы компрометации и тактики, техники и процедуры.
   - *Подключить команду реагирования на инциденты.* Завести заявку и назначить ее команде IR; при необходимости оказывать помощь в проведении расследования с учетом сложности инцидента.

ПРИМЕЧАНИЕ Даже при структурированном подходе охота идет не по прямой: будет множество поворотов и побочных заданий.

1.7. Обзор технологий и инструментов

Хотя охота за угрозами опирается на человеческий фактор, для успеха критически важен доступ к релевантным и надежным технологиям, а также к масштабируемым и гибким инструментам. События и действия можно собирать из конечных точек и с сетевых ресурсов, после чего отправлять в хранилища данных для дальнейшего анализа и поиска. Либо охотнику может понадобиться прямой доступ к артефактам и событиям из источников данных для выполнения поисков и расследований. Вот базовый набор технологий и инструментов подобного специалиста.

- *Активность конечных точек (серверов и рабочих станций).* Доступ к запускам процессов, сетевым портам, сведениям реестра (в Windows) и событиям доступа к системам — как правило, без этого не обойтись.

  Инструмент osquery (https://osquery.io) предоставляет охотникам доступ к данным конечных точек и позволяет писать SQL-запросы для получения данных от операционной системы. Аналогичные возможности есть у ряда открытых и платных EDR-систем.
- *Хранилища данных.* Системы для долговременного хранения событий и поиска. Обычно события из разных источников сети отправляют в хранилище вроде Splunk или Elasticsearch, доступное команде мониторинга безопасности и охотникам.
- *Аналитика.* Средства для масштабируемых поисков (например, в Splunk или Elasticsearch) и выполнения продвинутых функций — включая механизмы составления статистики и машинное обучение — на платформах наподобие Apache Spark.

В зависимости от исследуемой среды и задач охотника в арсенал могут входить и другие инструменты. Охотник может применять правила YARA (Yet Another Recursive Acronym) для выявления подозрительных действий на конечных точках и загружать правила Snort в сетевые средства безопасности (например, платформы IDS), чтобы перехватывать и анализировать подозрительный сетевой трафик.

В книге описан ряд бесплатных и платных инструментов, которыми пользуются охотники, а также показано, как применять их на практике. Кроме того, в приложении приведены инструкции по развертыванию некоторых из упомянутых инструментов.

Резюме

- Cyber Kill Chain включает семь этапов: разведку, вооружение, доставку, эксплуатацию, установку, командование и управление, выполнение действий.
- С ростом изощренности злоумышленников подход к ИБ должен быть проактивным.
- Структурированная охота — это подход, основанный на гипотезах: он нацелен на выявление угроз, которые не были обнаружены средствами детектирования, а также тех, что были обнаружены, но отклонены или недооценены человеком.
- Обнаружение угроз — реактивный подход к ИБ; охота — проактивный.
- Знание логики работы охотника и самого процесса охоты — ключ к успеху.
- Процесс охоты включает выработку гипотезы и попытку ее подтвердить. Если подтвердить не удается — гипотезу уточняют и повторяют поиск. Если гипотеза подтверждена — принимают меры против угрозы и расширяют поиск на другие системы и процессы.
- Для успешной охоты потребуются соответствующие навыки и инструменты для работы с конечными точками (серверов и рабочих станций), хранилищами данных и средствами аналитики.