

УДК 004.56
ББК 004.56
П32

Эндрю Пиз

П32 Активное выявление угроз с Elastic Stack: Построение надежного стека безопасности: предотвращение, обнаружение и оповещение / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2022. – 326 с.: ил.

ISBN 978-5-93700-116-0

Elastic Stack – мощный инструмент для предотвращения, обнаружения и реагирования на угрозы. Эта книга покажет, как наилучшим образом использовать его для обеспечения оптимальной защиты от киберугроз.

Вы ознакомитесь с основными компонентами Elastic Stack, освоите аналитические модели и методики целенаправленного поиска угроз и научитесь делиться логикой их обнаружения с партнерами и коллегами. Далее вы сможете развернуть Elastic Stack для мониторинга собственной сети и ресурсов, а также использовать панель визуализации данных Kibana для выявления злоумышленников в вашей сети.

Книга предназначена для всех читателей, которые интересуются тематикой активной кибербезопасности.

УДК 004.56
ББК 004.56

First published in the English language under the title «Threat Hunting with Elastic Stack – (9781801073783)»

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN (анг.) 978-1-80107-378-3
ISBN (рус.) 978-5-93700-116-0

Copyright ©Packt Publishing 2021
© Оформление, издание, перевод, ДМК Пресс, 2022

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. ТТП	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