Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Волгоградский государственный технический университет»
Факультет электроники и вычислительной техники
Кафедра «Электронно-вычислительные машины»

Контрольная работа
по дисциплине «Защита информации»
Организация централизованного сбора и анализа журналов
Вариант 10

Выполнил:
студент гр. ПрИн-466
Матвеев Степан Андеевич

Проверил:
к.т.н., доцент
Быков Дмитрий Владимирович

Волгоград 2025

I. Теоретическая часть

В современной ИТ-инфраструктуре логи - главный способ узнать, что происходит в системах: как работают сервисы, где возникают ошибки, фиксируются ли попытки несанкционированного доступа. Для централизованной работы с журналами применяется стек инструментов: OpenSearch, OpenSearch Dashboards, Logstash и Beats (в том числе Filebeat). Каждый компонент выполняет свою задачу; вместе они образуют единый конвейер сбора, обработки, анализа и визуализации данных.

OpenSearch - поисковый и аналитический движок, он служит ядром стека. Его назначение - хранить и быстро находить большие объёмы структурированных или полуструктурированных данных, в первую очередь логов. В ИТ-инфраструктуре OpenSearch разворачивают кластером из нескольких узлов; это обеспечивает отказоустойчивость и масштабируемость. Логи с серверов, приложений и сетевого оборудования поступают в OpenSearch в виде документов. У каждого документа есть поля: время события, уровень (info warning error), источник, текст сообщения и другие. Индексация позволяет выполнять сложные запросы за доли секунды: искать конкретные ошибки, фильтровать события по времени, агрегировать данные и выявлять аномалии. Для информационной безопасности это критично: именно здесь хранятся все журналы, нужные для расследования инцидентов и последующего аудита.

OpenSearch Dashboards - это веб-интерфейс для работы с данными, хранящимися в OpenSearch. Его удобно воспринимать как витрину над поисковым движком. В инфраструктуре администраторы, DevOps-инженеры и специалисты по информационной безопасности применяют его для анализа логов без необходимости писать сложные запросы вручную. Через Dashboards строят интерактивные панели, графики, таблицы и временные шкалы, которые отражают состояние системы в реальном времени. Например, визуализируют рост числа ошибок после релиза, нагрузку на сервисы или всплеск неудачных попыток входа. Для информационной безопасности Dashboards особенно полезен тем, что позволяет быстро заметить подозрительные паттерны: массовые ошибки аутентификации, обращения к несуществующим ресурсам, нетипичную активность в ночное время. Это ускоряет реакцию на инциденты и снижает вероятность того, что атака останется незамеченной.

Logstash выполняет роль промежуточного обработчика данных. Он находится между источниками логов и хранилищем OpenSearch и отвечает за приём, преобразование и обогащение событий. В реальной инфраструктуре логи часто имеют разный формат: текстовые файлы, JSON, syslog-сообщения, события Windows. Logstash приводит всё это к единому виду. С помощью фильтров он разбирает строки, извлекает нужные поля, приводит типы данных, добавляет геолокацию по IP-адресу или помечает события тегами. Logstash - это этап очистки и подготовки данных перед анализом. Для ИБ это

особенно важно, так как корректно разобранные и нормализованные логи значительно упрощают корреляцию событий, поиск цепочек атак и построение правил обнаружения инцидентов.
Elastic Beats - это лёгкие программы, которые ставятся прямо на серверы и другие узлы инфраструктуры. Они собирают данные и пересылают их дальше по конвейеру. Filebeat - один из самых популярных Beats. Он читает лог-файлы, работает как фоновый сервис, следит за изменениями в журналах и безопасно передаёт новые строки либо в Logstash, либо сразу в OpenSearch. Главная черта Filebeat - почти не тратит ресурсы машины и переживает сбои: если сеть исчезнет, данные не пропадут, а уйдут позже. Для информационной безопасности важно, что Filebeat постоянно и без задержек забирает логи с конечных систем, включая критичные серверы. Такой сбор снижает риск потери данных во время инцидента и делает журналы надёжным доказательством.

II. Практическая часть

1. Стек был развернут в Docker-контейнерах.

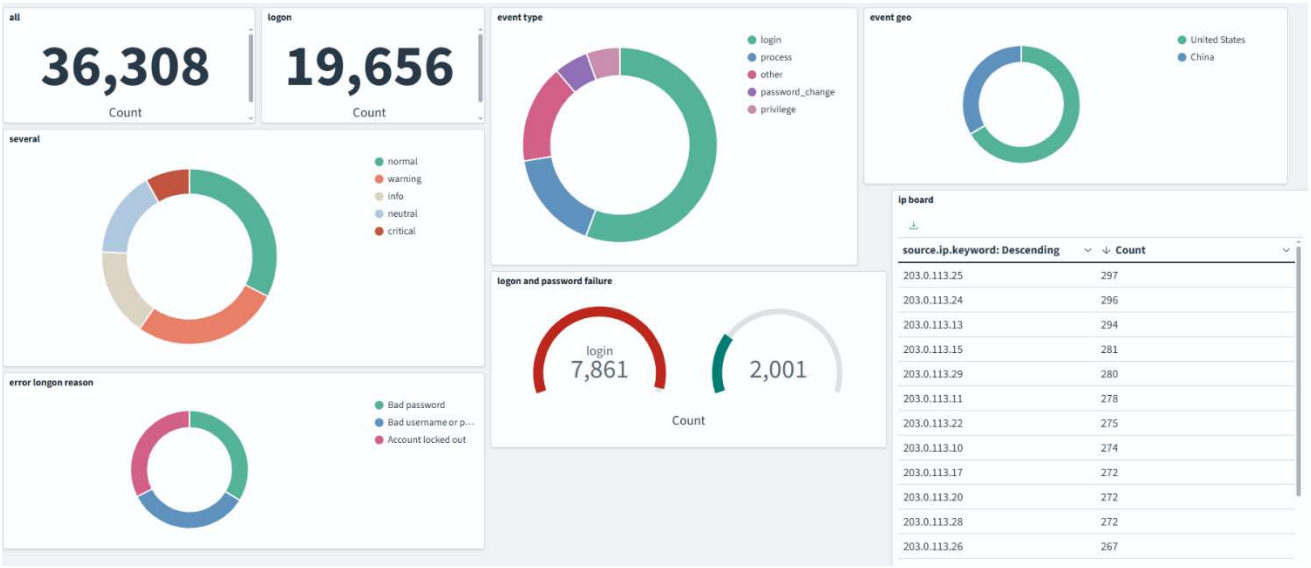
Образы:

- opensearchproject/opensearch:2.18.0
- opensearchproject/opensearch-dashboards:2.18.0
- public.ecr.aws/opensearchproject/logstash-oss-with-opensearch-output-plugin:8.4.0
- docker.elastic.co/beats/filebeat:8.10.0

2. Описание датасета:
    a. Логи windows security – логи многострочные
    b. Примерно 36000 логов

3. Стек настраивается при помощи docker compose:
    a. Opensearch – работает на порте 9200 с паролем
    b. Opensearch dashboard – на порте 5601
    c. Logstash – на порте 5044
    d. Filebeat

4. Скриншоты
    a. Dashboard


all
36,308
Count
logon
19,656
Count
event type
login
process
other
password_change
privilege
event geo
United States
China
several
normal
warning
info
neutral
critical
error longon reason
Bad password
Bad username or p...
Account locked out
logon and password failure
login
7,861
2,001
Count
ip board
source.ip.keyword: Descending
Count
203.0.113.25 297
203.0.113.24 296
203.0.113.13 294
203.0.113.15 281
203.0.113.29 280
203.0.113.11 278
203.0.113.22 275
203.0.113.10 274
203.0.113.17 272
203.0.113.20 272
203.0.113.28 272
203.0.113.26 267

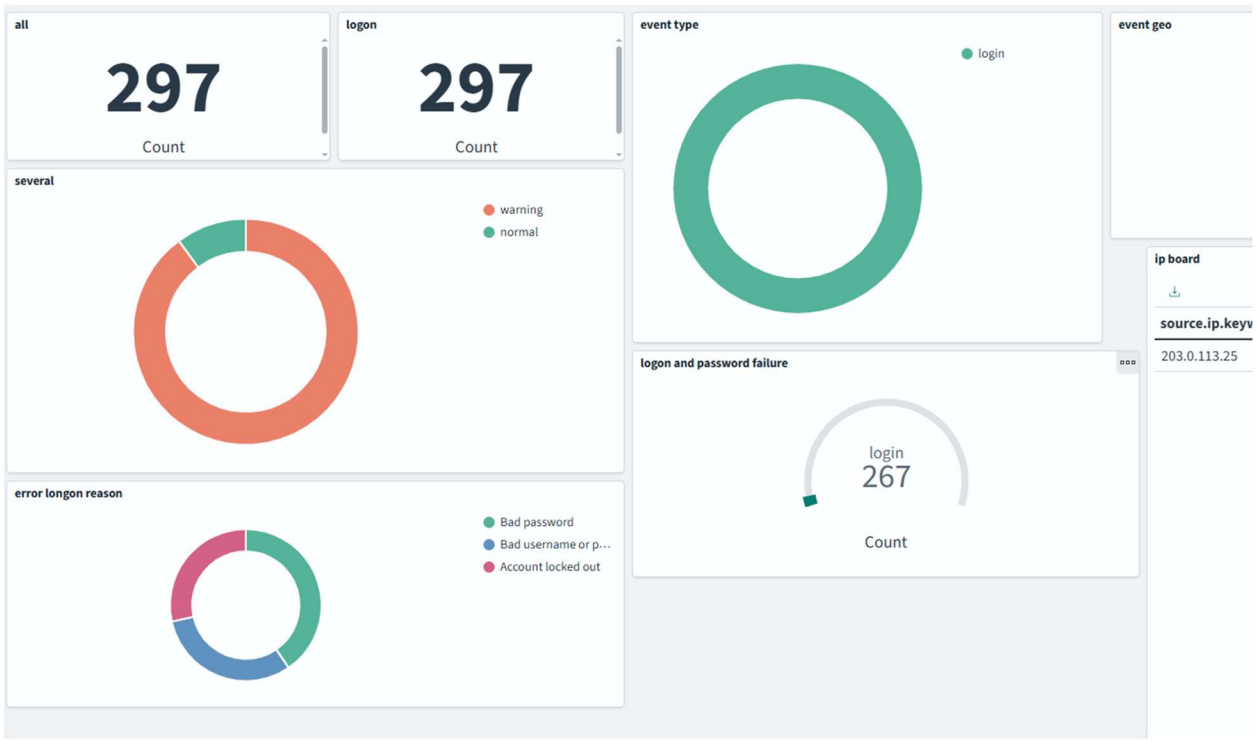
b. Discover

t	event.original	2025-03-26 23:59:53 WIN-FILE01 Security 4688 A new process has been created. Subject: Security ID: S-1-5-21-2851687098-1894345498-1991382139-1065 Account Name: charlie Account Domain: LAB Logon ID: 0x61d4d New Process:
t	event_action	create
t	event_id	4688
t	event_message	A new process has been created
t	event_result	success
t	event_type	process
t	host.name	2e76ef2bb4fc
t	host_name	WIN-FILE01
t	input.type	log
t	log.file.path	/data/variant06_windows_security.log
t	log.flags	multiline
#	log.offset	8,376,104
t	log_source	Security
t	log_timestamp	2025-03-26 23:59:53
t	log_type	windows-security
t	message	2025-03-26 23:59:53 WIN-FILE01 Security 4688 A new process has been created. Subject: Security ID: S-1-5-21-2851687098-1894345498-1991382139-1065 Account Name: charlie Account Domain: LAB Logon ID: 0x61d4d New Process:
t	severity	info
t	severity_color	blue

c. Logstash

```
grok {
   match => {
    "message" => [
     "Failure
Information:\s+Status:\s+%{BASE16NUM:errlogon.failure_status}\s
+Sub Status:\s+%{BASE16NUM:errlogon.failure_sub_status}"
    ]
   }
   tag_on_failure => []
  }
```

5. Краткий анализ
    a. Подозрительные события
    b. Почти все попытки входа провалились с одного ip



III. Задания повышенной сложности

1. Filebeat Используется для сборки события из многострочного лога:
```
….
  multiline.type: pattern
  multiline.pattern: '^\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}'
  multiline.negate: true
  multiline.match: after
….
output.logstash:
  hosts: ["logstash:5044"]
```

2. Geoip logstash используется для обогащения события позицией, городом и страной:
```
  geoip {
    source => "source.ip"
    target => "source"
    database => "/usr/share/logstash/GeoLite2-City.mmdb"
```

```
  tag_on_failure => []
}
```