Лабораторная работа 3

**Атака bruteforce протокол RDP**

## **Задача**

* Провести bruteforce атаку на Windows устройство с целью получения доступа.
* Написать правило для обнаружения компьютерной атаки

## **Общие сведения и сценарии**

В ходе данной лабораторной работы студенты узнают, как проводить bruteforce атаки с помощью утилиты crowbar, а также научатся писать правила для обнаружения компьютерных атак на основе событий Windows.

Атака будет проводиться с компьютера злоумышленника (Kali Linux) на устройство под управлением ОС Windows 7. События, созданные во время и после атаки отправляются на ВМ Server, где аналитик информационной безопасности увидит оповещение о происходящей атаке.

## **Необходимые ресурсы**

ПК или ноутбук с доступом к Интернету и настроенным лабораторным стендом.

## **Ход выполнения лабораторной работы**

### Шаг 1 - Запуск стенда

Для выполнения данной лабораторной работы понадобятся следующие ВМ: Kali Linux, Server, Windows 7

### Шаг 2 - Установка Crowbar

Ввести следующую команду в терминал ВМ Kali Linux: sudo apt install crowbar

### Шаг 3 - Проведение атаки

После установки утилиты Crowbar необходимо запустить подбор пароля: crowbar --server 192.168.128.52/32 -b rdp -u IKTZ-93 -C passwords.txt (Рисунок 1)

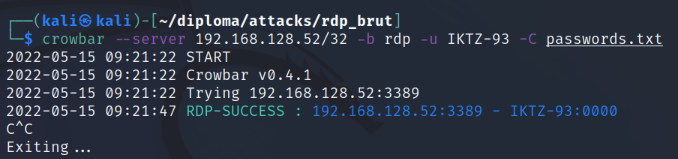


Рис. 1. Использование утилиты Crowbar

### Шаг 4 - Анализ событий и написание правила по обнаружению атаки.

Перейдя на вкладку “Security”->”Hosts”, можно увидеть большое количество ложных попыток авторизации (Рисунок 2).

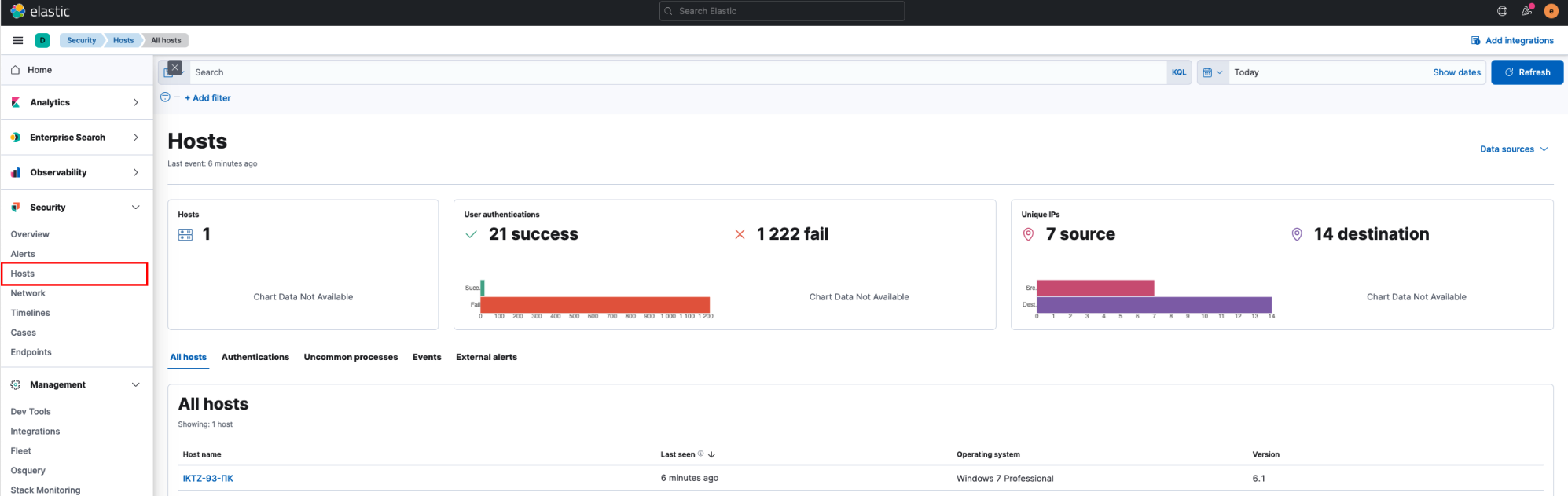


Рис. 2. Вкладка “Hosts”

Для дальнейшего анализ атаки перейдем на вкладку “Discover”. Среди большого числа различных событий нас интересуют события с event\_id 4625 (Неудачная попытка входа), 4624 (Успешная попытка входа), 1149 (Службы удаленных рабочих столов: Успешная проверка подлинности пользователя).

Можно заметить, что появилось большое количество логов с event\_id 4625, это связано с тем, что программа crowbar перебирает множество паролей с намерением подобрать верный. Так как наша атака прошла успешна, нашей целью будет найти среди всех событий логи с event\_id 4624 или 1149. Однако события 4624 генерируются не только при успешной авторизации по протоколу RDP, но также и при обычном входе в систему, по этой причине мы обратим внимание на события с event\_id 1149.

Найти логи с event\_id 1149 можно при помощи поискового запроса в верхней части интерфейса: winlog.event\_id : 1149 (Рисунок 3)

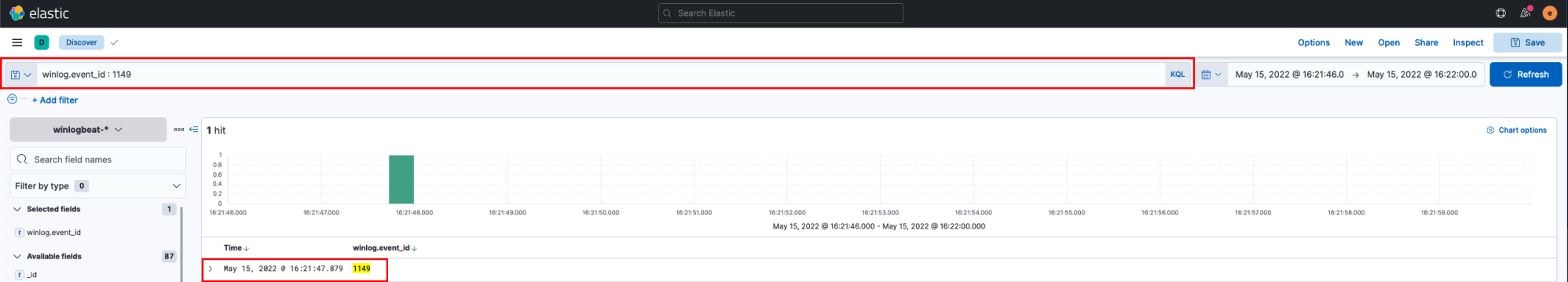


Рис. 3. Поиск события 1149

Обратим внимание на время появления события, это поможет нам в поисках лог-файла с event\_id 4624. В правой верхней части интерфейса указываем временные рамки показываемых событий (Рисунок 4). Далее вводим следующий запрос для фильтрации выдаваемых логов winlog.event\_id : 4625 or winlog.event\_id : 4624 or winlog.event\_id : 1149. Видно, что идет несколько подряд событий с event\_id 4625, затем одно с 4624, и с 1149. Таким образом мы можем понять, что произошла атака по подбору пароля для подключения по протоколу RDP.

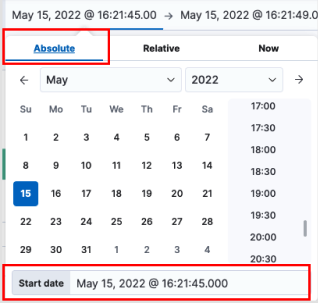


Рис. 4. Редактирование временных рамок

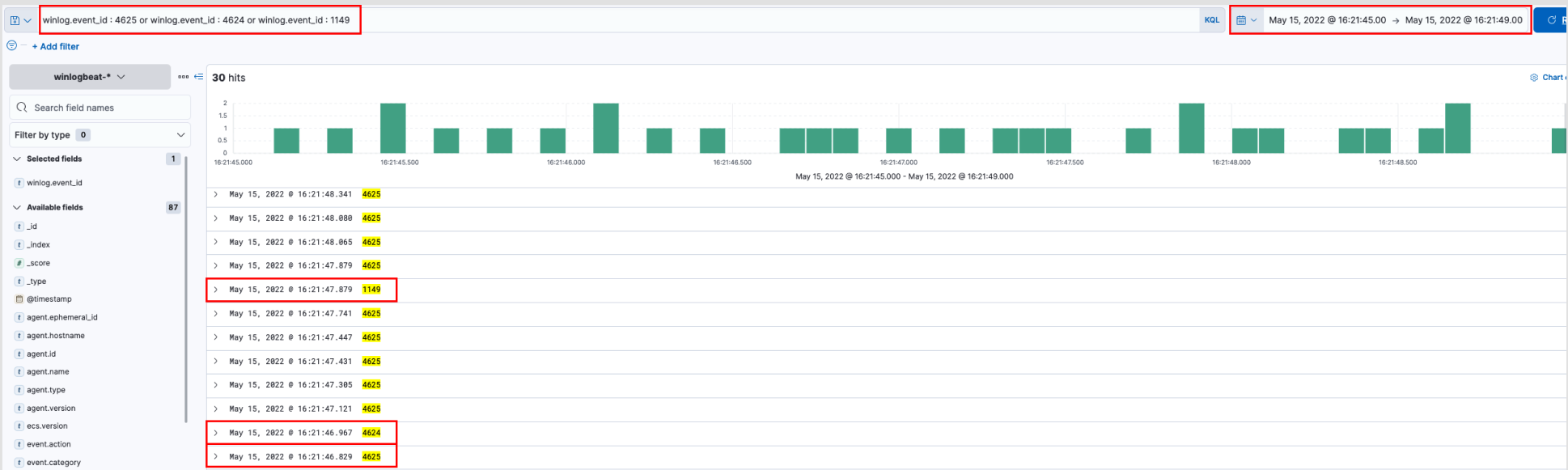


Рис. 5. Фильтрация результатов выдачи

Теперь, зная, в каком порядки и какие события появляются при атаке bruteforce, мы можем автоматизировать их обнаружение. Для этого переходим на вкладку “Security”->”Rules” и нажимаем кнопку “Create new rule” (Рисунок 6).

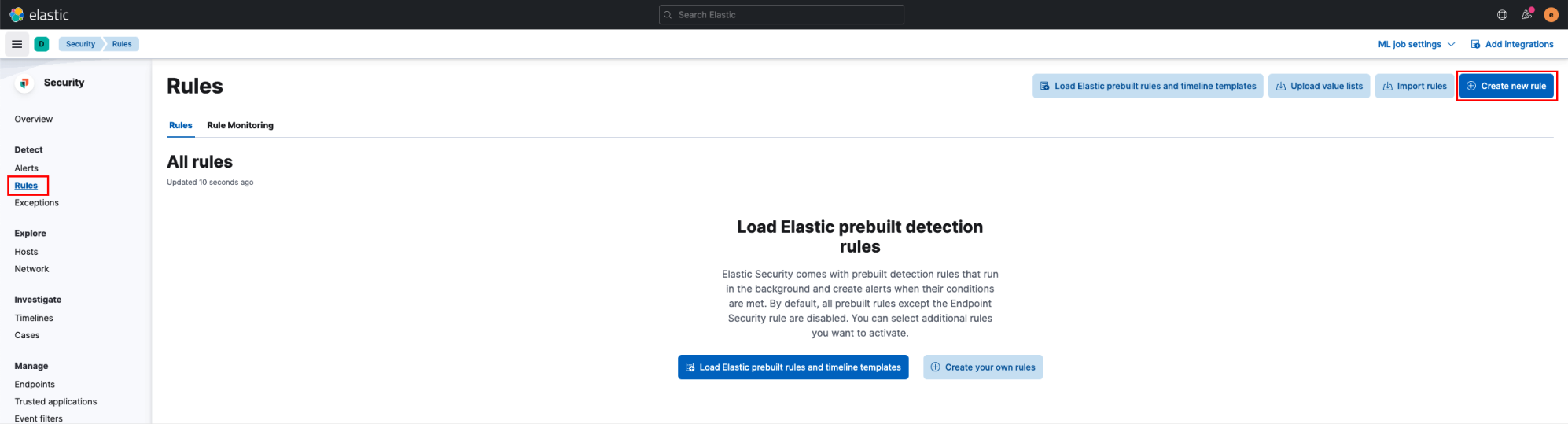


Рис. 6. Создание правила

Выбираем Event Correlation, из индексов убираем все, кроме winlogbeat и пишем следующий запрос:

sequence

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4625]

[authentication where winlog.event\_id == 4624]

[any where winlog.event\_id == 1149]

(Рисунок 7).

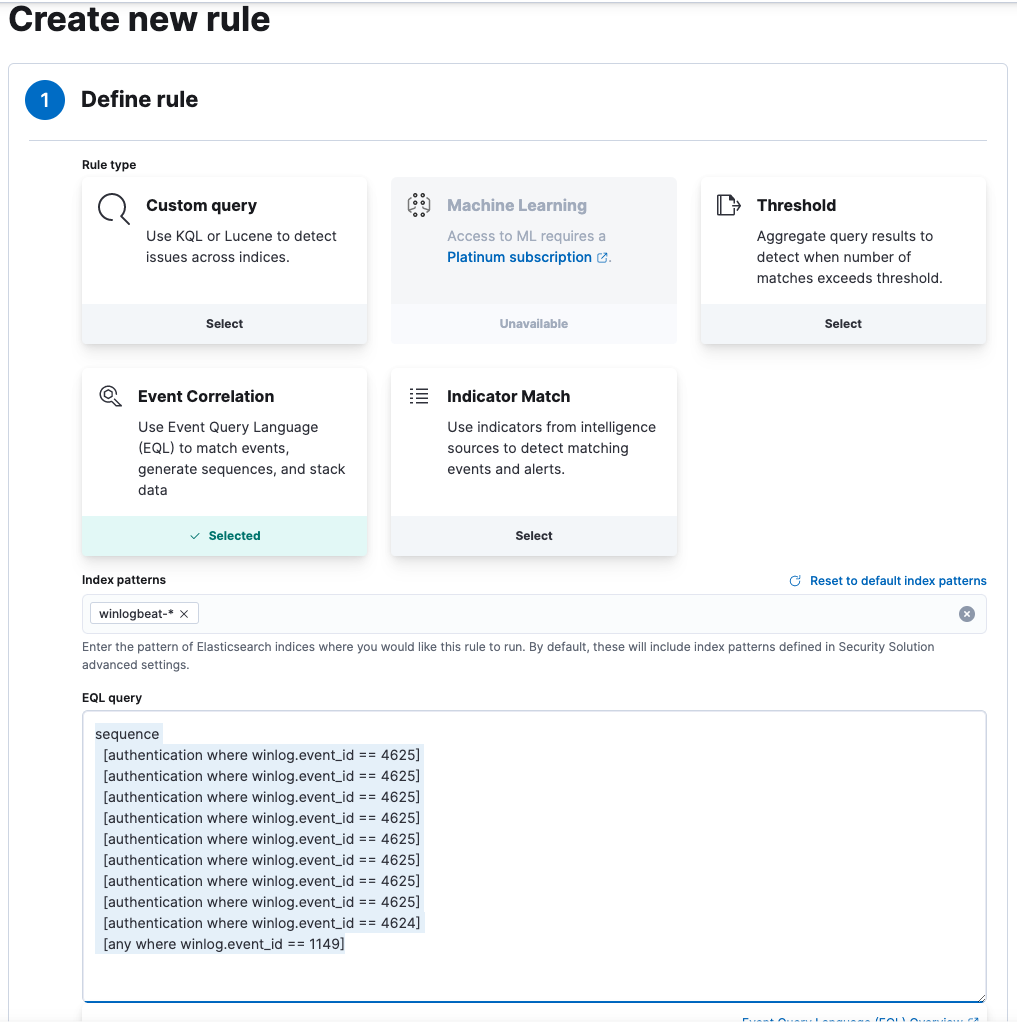


Рис. 7. Создание правила

Для проверки правила необходимо выбрать “Last day”, если в совершали атаку больше часа назад, и нажать кнопку “Preview results”, как показано на рисунке 8.

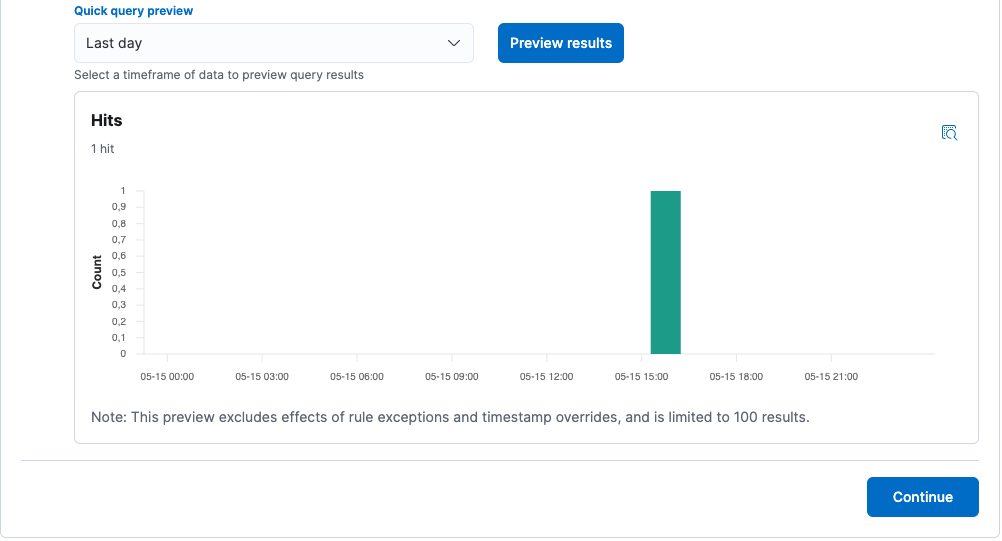


Рис. 8. Проверка работы правила

Далее заполняем поля “Name”, “Description” и “Default severity” (Рисунок 9).

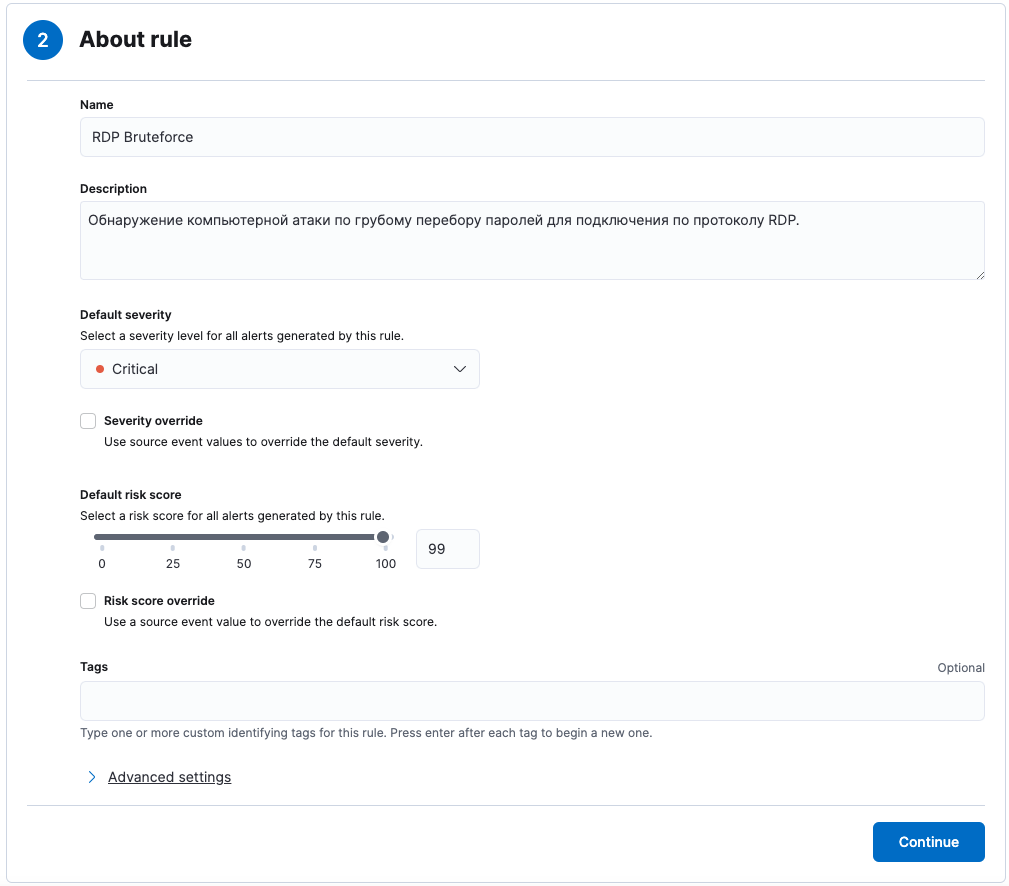


Рис. 9. Создание правила

Указываем, что правило должно запускаться каждую минуту (Рисунок 10). И заканчиваем создание правила нажав на кнопку “Create & activate rule”.

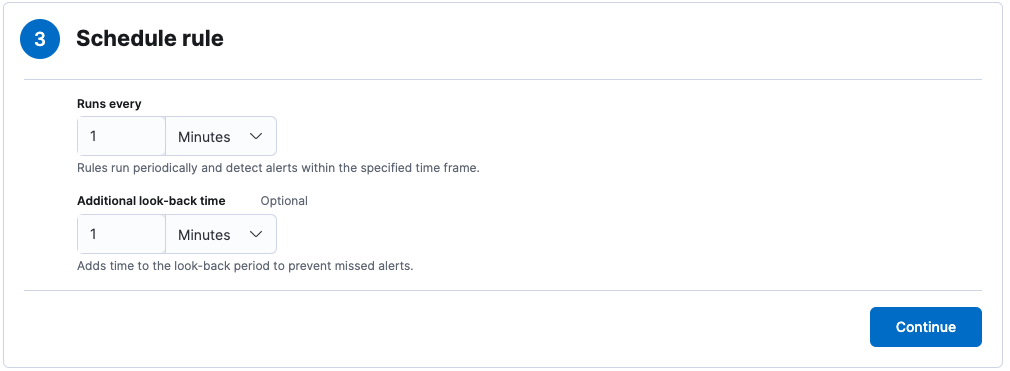


Рис. 10. Создание правила