UI. Unknown Impact

АПРЕЛЬ 8, 2022

AITU HACKDAY CHALLENGE

TRANSFER LOGS FROM EMAIL TO THE PLATFORM

EMAIL2THEHIVE

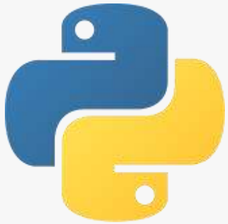
ЗАДАНИЕ ОТ KAZDREAM

ZUFAR IDOYATOV, MUKHAMBET NAZAROV, ALIBEK AKHMETOV, BEKZHAN DARMENOV

РЕШЕНИЕ

В качестве решения было принято написать Scrapper на языке Python, для передачи журнала событий из письма на TheHive платформу.

DigitalOcean



СТЕК ТЕХНОЛОГИЙ

DASHBOARD
ПРЕДВАРИТЕЛЬНАЯ РАБОТА

http://46.101.216.236:9000/

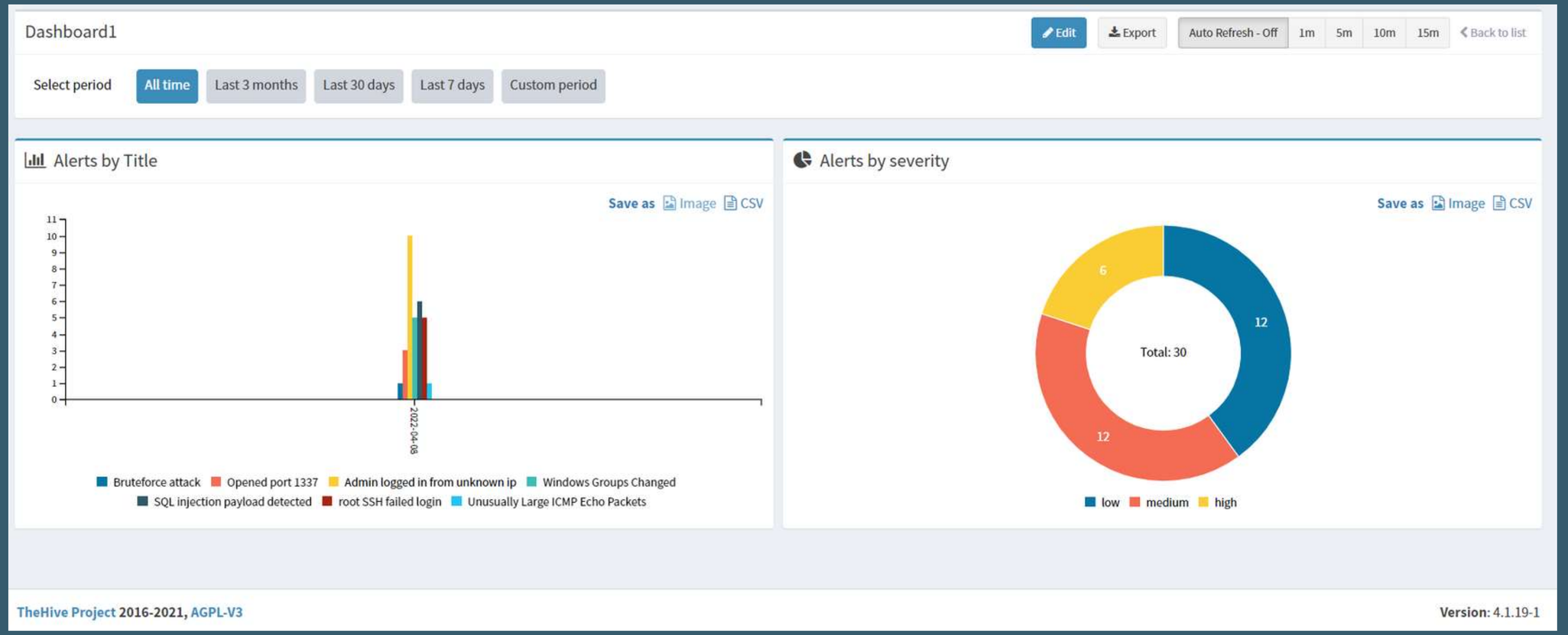


Рисунок 1. Панель мониторинга TheHive платформы

DASHBOARD
ПРЕДВАРИТЕЛЬНАЯ РАБОТА

http://46.101.216.236:9000/

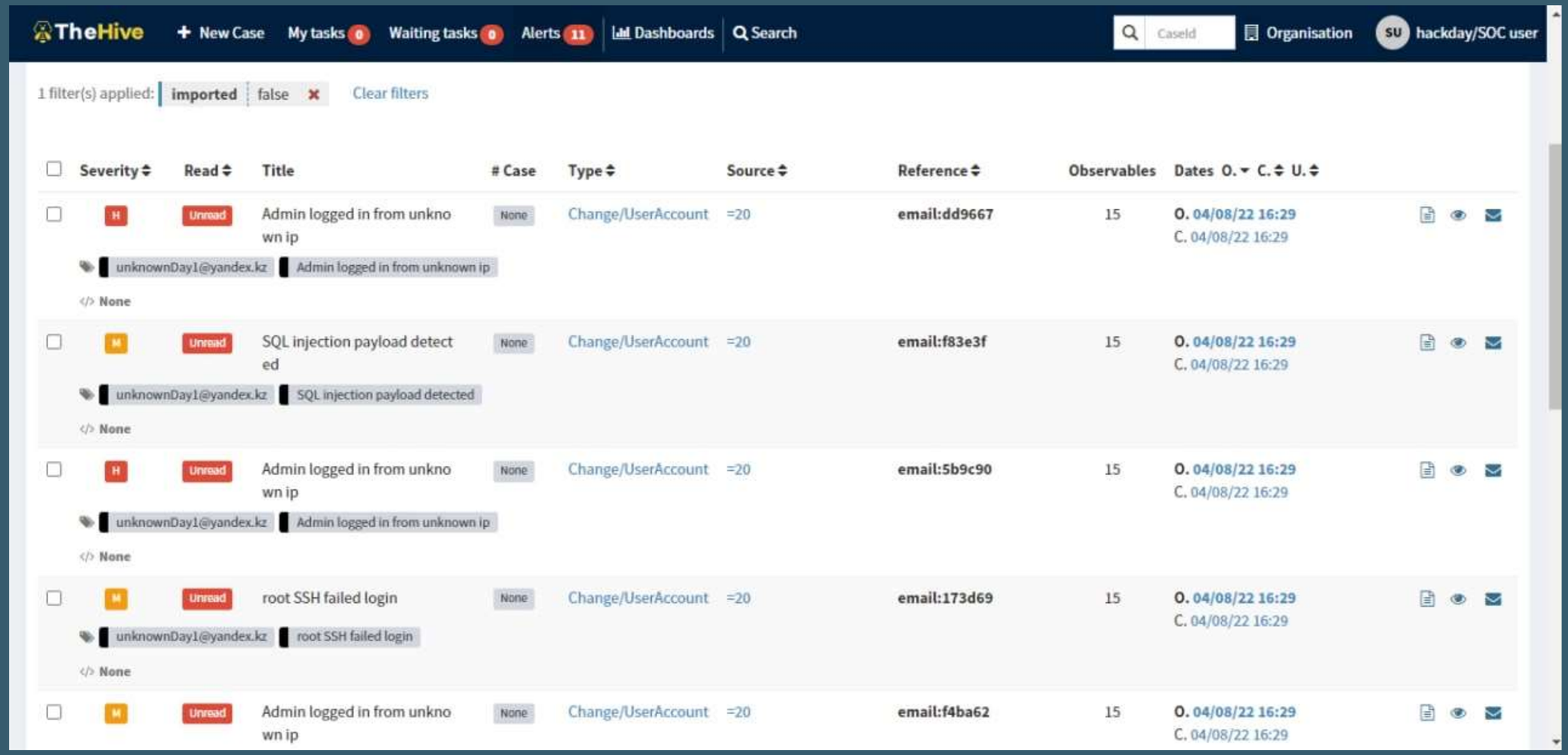


Рисунок 2. Список событий TheHive платформы

ПРОЕКТ КОДА

```python
def parse_text(text):
    text = text
    if re.search('Incident ID:', text) == None:
        return None

    event_info = {}

    raw_loc = text.find('Raw Events')
    # list of {Info}: {Event}
    event_list = re.findall(r"[\w| ]*:[\w|\S_| ]*", text[:raw_loc])

    for content in event_list:
        content = content.strip().split(':')

        key = content[0]
        value = content[1:]
        value = ':'.join(value).strip()
        event_info[key] = value
        url = re.findall(r'https?:[0-9]+(?:\.[0-9]+){3}[-a-zA-Z0-9@:%._\+~#=]{1,256}\.[a-zA-Z0-9()]{1,6}\b([-a-zA-Z0-9()@:%_\+.~#?&//=]*)', value)
        if url != []:
            event_info[key] = url[0]

    names_dict = {
        'title': ['incident title', 'title', 'event title'],
        'severity': ['event severity', 'severity', 'incident severity'],
        'date': ['date', 'incident first occurrence time', 'incident last occurrence time',
                 'time', 'timestamp', 'datetime', 'occurrence time', 'event occurrence time',
                 'incident occurrence time', 'event first occurrence time', 'event last occurrence time'],
        'status': ['status', 'incident status', 'event status'],
        'type': ['type', 'event type', 'incident type', 'category', 'incident category', 'event category'],
        'source': ['host ip', 'source ip', 'source address'],
    }
```

Рисунок 3. Фрагмент кода с парсингом логов

Рисунок 4. Архитектура

ВЕКТОР ПРОДВИЖЕНИЯ

- Проработать систему логирования событий
- Провести различные нагрузочные тесты для выявления аномалий
- Сделать систему оповещения при выявлении событий со статусом: critical
- Добавить whitelist систему для доменов и IP адресов отправителей писем
- Проработать функции отправки событий посредством писем с TheHive платформы

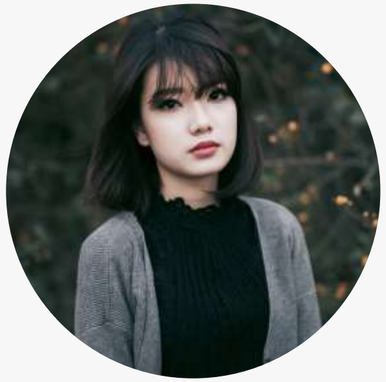
@unknownimpact

НАША КОМАНДА

ASTANA IT UNIVERSITY

MUKHAMBET NAZAROV

Security Analyst
Student



ALIBEK AKHMETOV

Security Analyst
Student

ZUFAR IDOYATOV

MLOp
Student

BEKZHAN DARMENOV

Security Analyst
Student