



## **МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

---

**Институт кибербезопасности и цифровых технологий (ИКБ)**

---

**КБ-2 «Информационно-аналитические системы кибербезопасности»**

---

### **ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №13**

**В РАМКАХ ДИСЦИПЛИНЫ «ПРИНЦИПЫ ПОСТРОЕНИЯ,  
ПРОЕКТИРОВАНИЯ И ЭКСПЛУАТАЦИИ  
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ»**

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

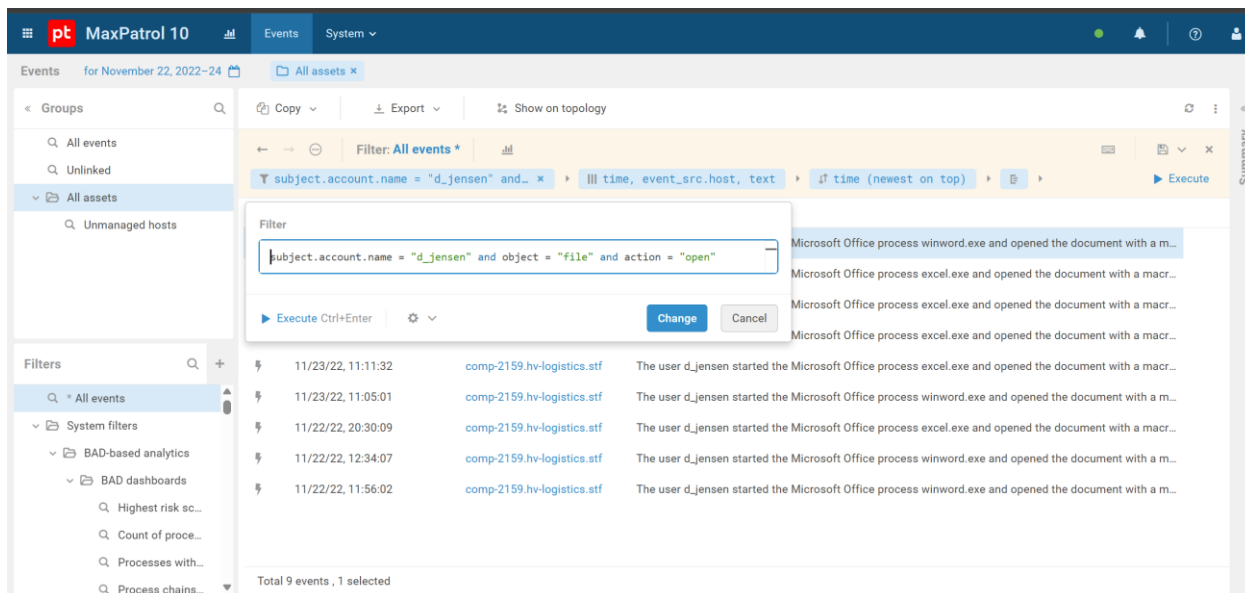


Рисунок 1 – фильтр

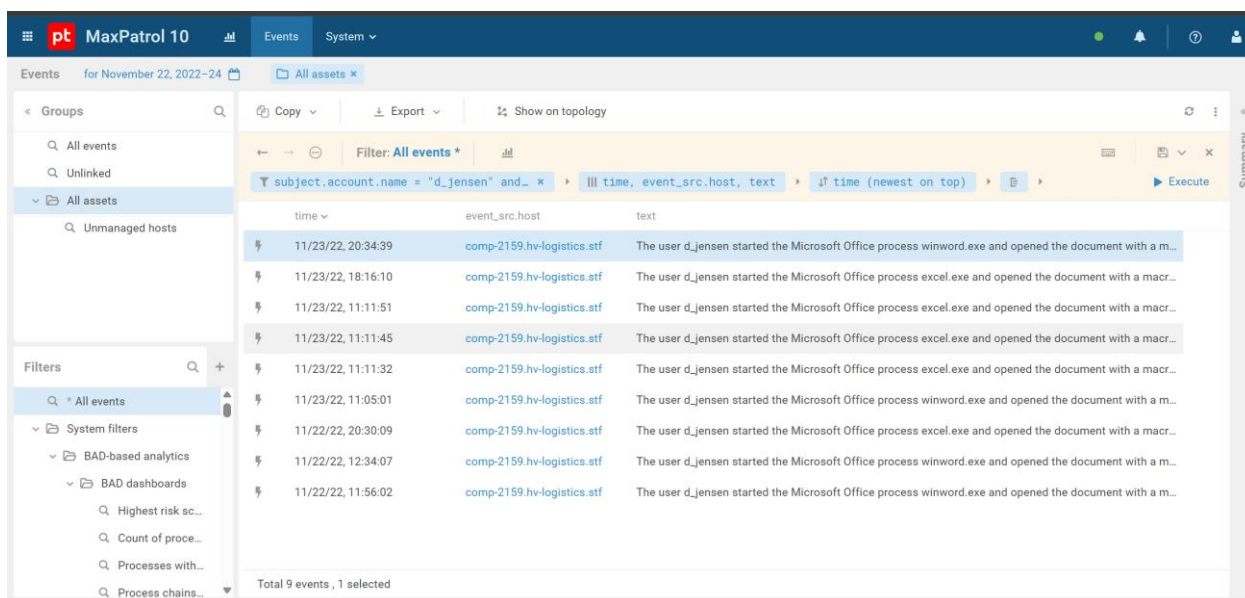


Рисунок 2 - результат вывода

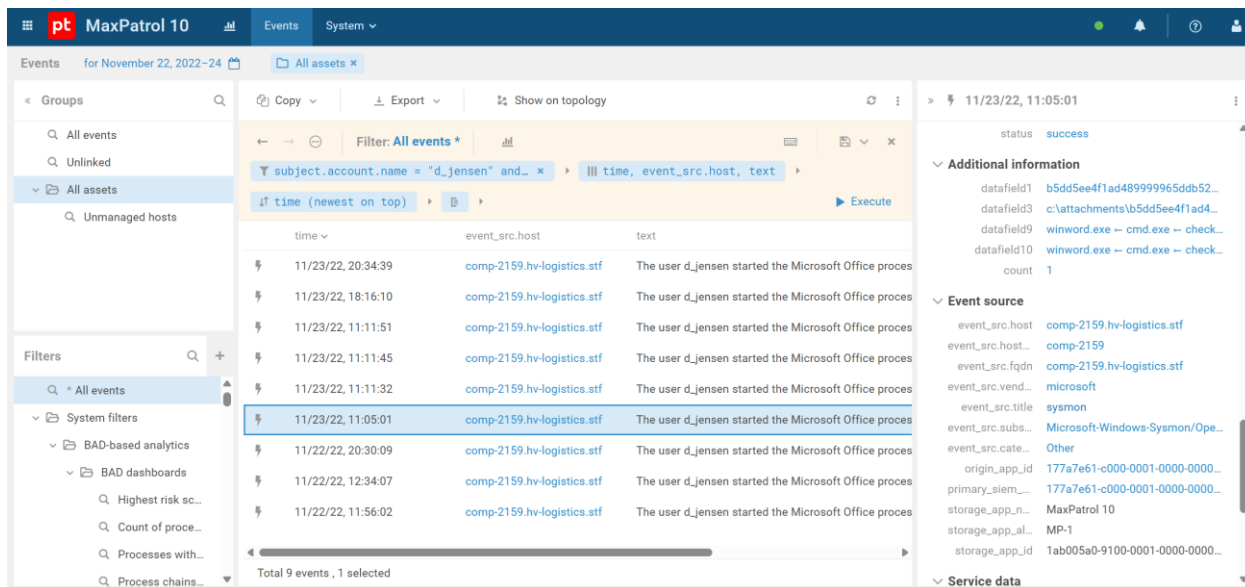


Рисунок 3- открытие документа

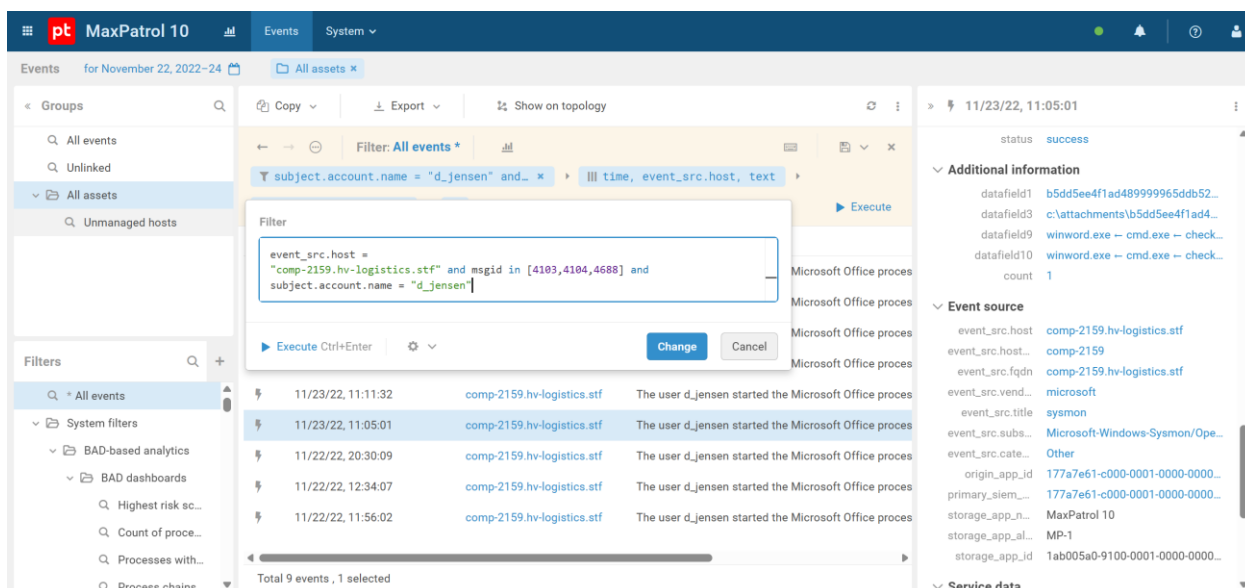


Рисунок 4 - новый фильтр, на основе полученных данных

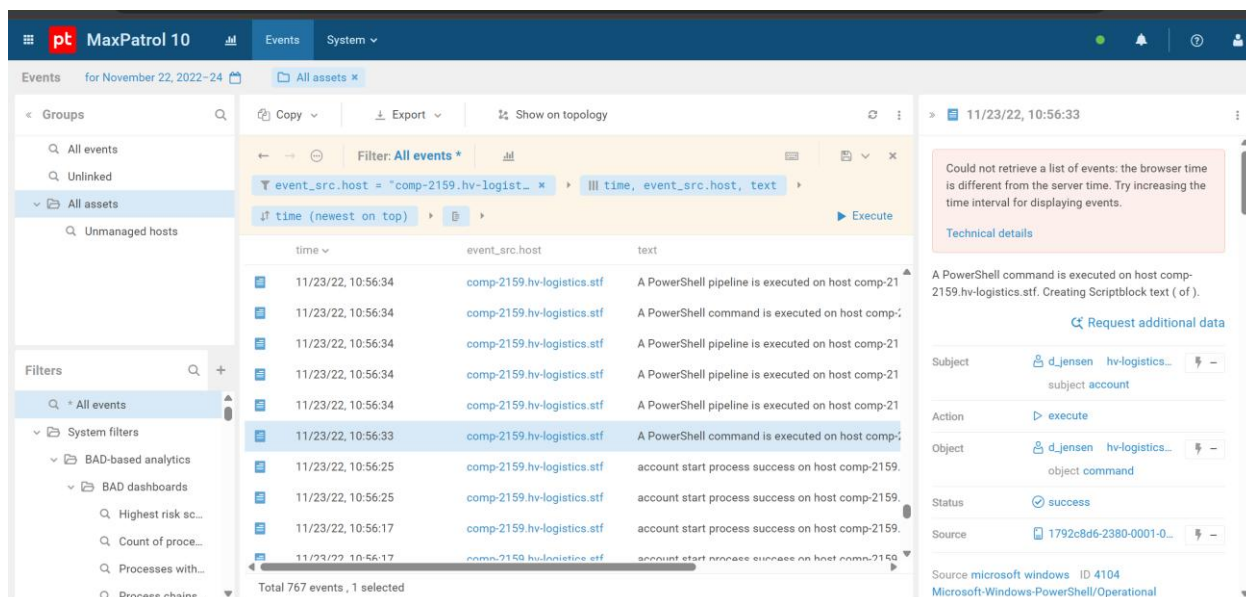


Рисунок 5 - команда, скачивающая powershell скрипт

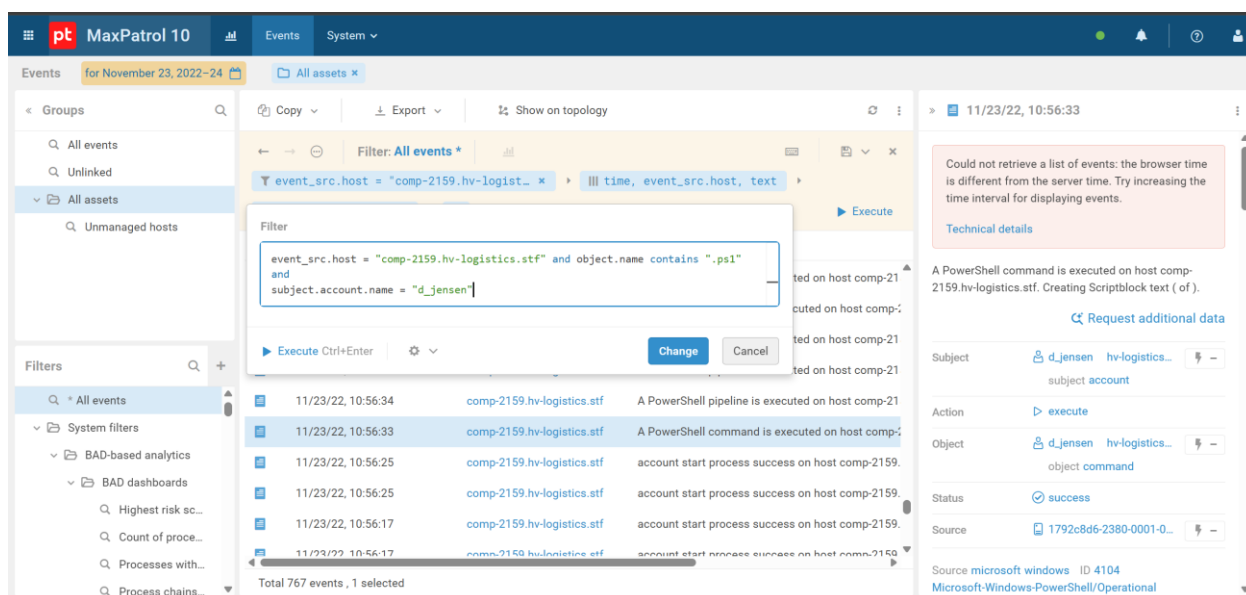


Рисунок 6 - новый фильтр

MaxPatrol 10

Events System

Events for November 23, 2022-24 All assets

Groups

- All events
- Unlinked
- All assets
  - Unmanaged hosts

Filters

- All events
- System filters
- BAD-based analytics
- BAD dashboards
  - Highest risk sc...
  - Count of proce...
  - Processes with...
  - Process chains...

Copy Export Show on topology

Filter: All events \*

event\_src.host = "comp-2159.hv-logistics.stf" time, event\_src.host, text

time (newest on top)

time	event_src.host	text
11/23/22, 11:57:32	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:57:16	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:41:42	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:32:21	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 11:10:09	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 10:57:21	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 10:57:21	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma
11/23/22, 10:57:20	comp-2159.hv-logistics.stf	The user d_jensen attempted to run the script "qwe.ps1"
11/23/22, 10:57:20	comp-2159.hv-logistics.stf	The user d_jensen attempted to run the script "qwe.ps1"
11/23/22, 10:56:18	comp-2159.hv-logistics.stf	User d_jensen from host created the potentially ma

Total 34 events, 1 selected

11/23/22, 10:57:20

The user d\_jensen attempted to run the script "qwe.ps1" on host comp-2159.hv-logistics.stf

Request additional data

Subject d\_jensen hv-logistics.stf subject account

Action execute

Object powershell.exe object file\_object fullpath c:\windows\syswow64\qwe.ps1 object file\_object type script fullpath c:\windows\tasks\qwe.p...

Status success

Source 1792c8d6-2380-0001-0...

Source microsoft windows ID Security Category Attack / Execution / Command and Scripting Interpreter

Рисунок 7 - alert.key