



## **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 №10**

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

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

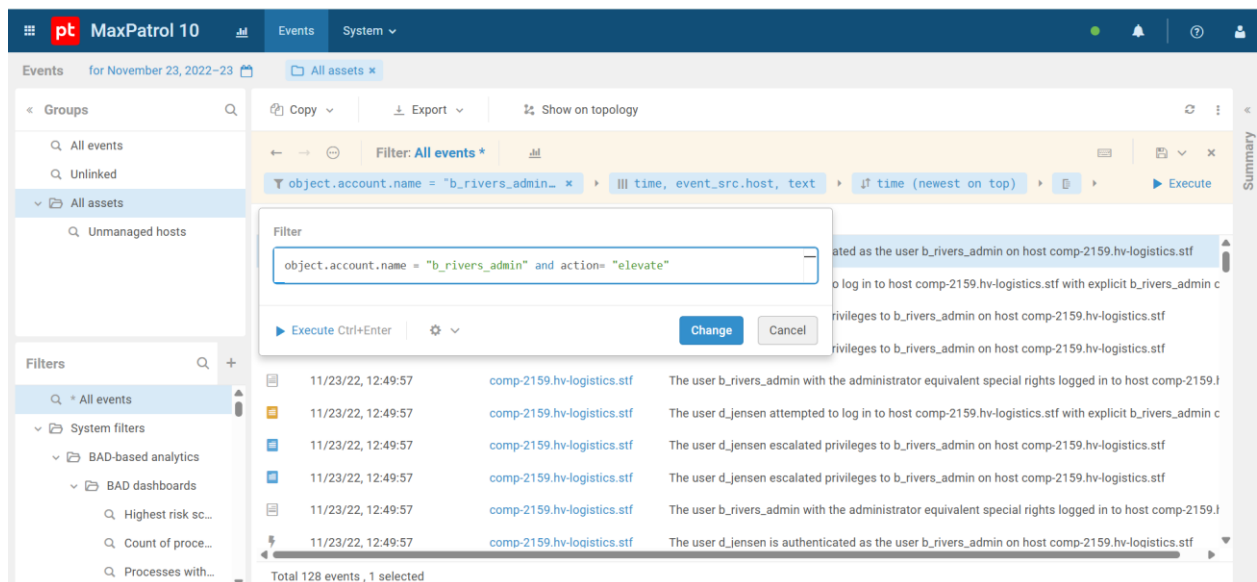


Рисунок 1 - Первичный фильтр

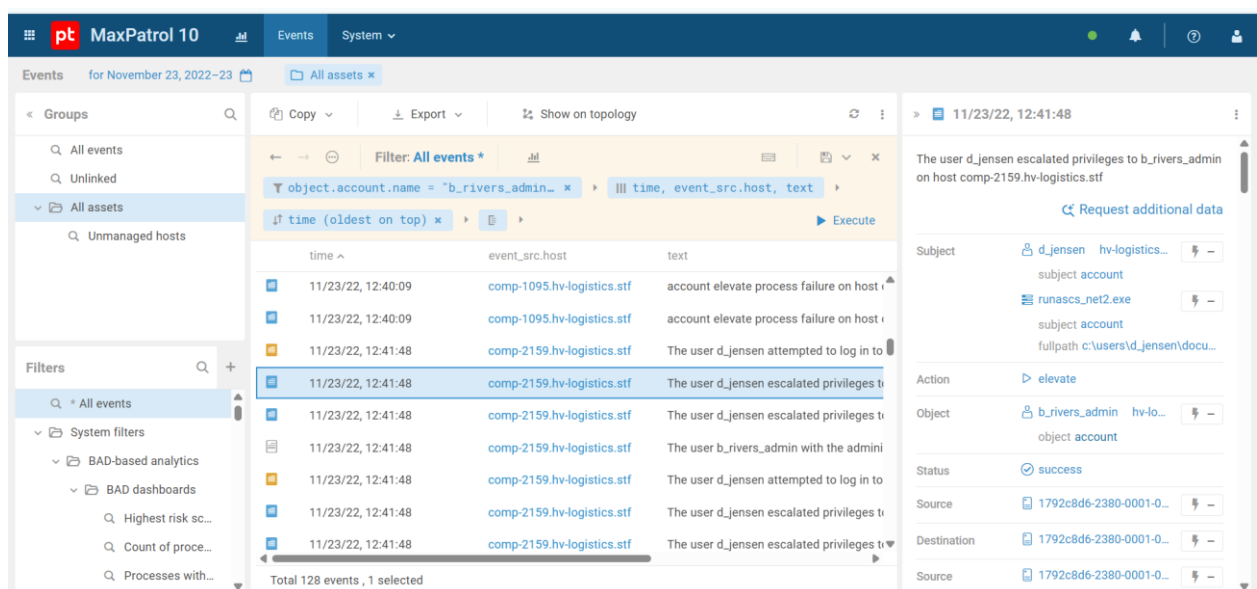


Рисунок 2 - повышение привелегий

✓

Heavy Logistics (2022)

○

Низкий уровень сложности

100 баллов

получено

↑

### Небезопасное хранение данных / Задание 7.1

Задание

В транспортной компании Heavy Logistics проблемы с выполнением требований парольной политики и с надежным хранением аутентификационных данных.

Однажды администратор Boyd Rivers оставил файл с паролем своей доменной учетной записи (b\_rivers\_admin) на компьютере одного из эйчаров: забыл удалить его после настройки. В результате фишинговой атаки злоумышленники получили доступ к устройству эйчара, нашли этот файл и воспользовались данными для повышения привилегий (23 ноября 2022 года с 09:30 по 09:50 UTC).

Укажите имя рабочей станции эйчара, на которой хранится файл с паролем.

Тактики, техники и подтехники атак по MITRE ATT&CK

- TA0006. Получение учетных данных | T1552. Незащищенные учетные данные | T1552.001. Учетные данные в файлах

Средства защиты

MaxPatrol SIEM

Принятый ответ

comp-2159.hv-logistics.stf

Дата и время проверки

29 октября, 16:55

Рисунок 3 - первый ответ

The screenshot shows the MaxPatrol 10 SIEM interface. On the left, there's a sidebar with 'Groups' and 'Filters'. The main area displays a list of events for November 23, 2022. A filter dialog box is open, showing a filter rule: `event_src.host = "comp-2159.hv-logistics.stf" and object.name = "runascs_net2.exe" and subject.account.name = "d_jensen" and object.process.cmdline contains "b_rivers_admin"`. The dialog has 'Execute Ctrl+Enter', 'Change', and 'Cancel' buttons. On the right, a detailed view of a selected event is shown, including fields like `object.path`, `object.hash`, `object.account.name`, `object.account.domain`, `object.pcount.fullname`, `object.session_id`, `object.account.id`, `object.process.name`, `object.process.path`, `object.original_name`, `object.process.fullpath`, `object.process.cmdline`, `object.process.guid`, `object.process.id`, `object.process.hash`, `object.process.version`, `object.process.cwd`, `object.process.parent.name`, `object.process.parent.path`, and `object.process.parent.fullpath`.

Рисунок 4 - второй фильтр

»	11/23/22, 12:41:22	
object.path	c:\users\d_jensen\documents\	
object.hash	340CC46BA058C2E554AF2431ADA7FB242AC7B6C6...	
object.account.name	d_jensen	
object.account.domain	hv-logistics.stf	
object.account.fullname	d_jensen@hv-logistics	
object.account.session_id	1342507	
object.account.id	S-1-5-21-794427356-1309637812-1474570248-1152	
object.process.name	runascs_net2.exe	
object.process.path	c:\users\d_jensen\documents\	
object.process.original_na...	RunasCs_net2.exe	
object.process.fullpath	c:\users\d_jensen\documents\runascs_net2.exe	
object.process.cmdline	RunasCs_net2.exe B_Rivers_admin -p zY2oWqz2qn3Ne71W -d hv-logistics.stf	
	^ Collapse	
object.process.guid	076CA06C-EAC2-637D-481E-000000003100	
object.process.id	5468	
object.process.hash	SHA256:340CC46BA058C2E554AF2431ADA7FB242A...	
object.process.version	0.0.0.0	
object.process.cwd	C:\Users\D_Jensen\Documents\	
object.process.parent.name	cmd.exe	
object.process.parent.path	c:\windows\system32\	
object.process.parent.fullp...	c:\windows\system32\cmd.exe	

Рисунок 5 - пароль администратора

✓

Heavy Logistics (2022)

Низкий уровень сложности

100 баллов

получено

Небезопасное хранение данных / Задание 7.2

Задание

В транспортной компании Heavy Logistics проблемы с выполнением требований парольной политики и с надежным хранением аутентификационных данных.

Однажды администратор Boyd Rivers оставил файл с паролем своей доменной учетной записи (b\_rivers\_admin) на компьютере одного из эйчаров: забыл удалить его после настройки. В результате фишинговой атаки злоумышленники получили доступ к устройству эйчара, нашли этот файл и воспользовались данными для повышения привилегий (23 ноября 2022 года с 09:30 по 09:50 UTC).

Приведите пароль учетной записи b\_rivers\_admin.

Тактики, техники и подтехники атак по MITRE ATT&CK

1. TA0004. Повышение привилегий | T1078. Существующие учетные записи | T1078.002. Доменные учетные записи

Средства защиты

MaxPatrol SIEM

Принятый ответ

Дата и время проверки

zY2oWqz2qn3Ne71W

29 октября, 17:12

Рисунок 6 - второй ответ

pt

MaxPatrol 10

Events

System

Events

for November 22, 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...

Copy

Export

Show on topology

11/22/22, 20:25:09

Filter: All events \*

event\_src.host = "comp-2159.hv-logisti..."

Filter

event\_src.host = "comp-2159.hv-logistics.stf" and object.process.parent.cmdline contains "C:\Attachments" and (object.process.parent.cmdline contains ".doc" or object.process.parent.cmdline contains ".xls") and action = "start" and subject.account.name = "d\_jensen" and object.process.parent.cmdline not contains ".doc" and object.process.parent.cmdline not contains "wiword.exe"

Execute Ctrl+Enter

Change

Cancel

11/23/22, 18:11:10

comp-2159.hv-logistics.stf

account s

Total 5 events, 1 selected

datafield9

C:\Windows\system32\cmd.exe /c "start C:\Attachmen

ts\76bcf5a5e7b44630b01b9821db94c360book\_withco

b.xls"

Collapse

datafield10

excel.exe -- cmd.exe -- checker.exe -- checker.exe --

msgid

1

event\_src.host

comp-2159.hv-logistics.stf

\_src.hostname

comp-2159

event\_src.fqdn

comp-2159.hv-logistics.stf

event\_src.vendor

microsoft

event\_src.title

sysmon

event\_src.subsys

Microsoft-Windows-Sysmon/Operational

event\_src.rule

-

event\_src.category

Other

origin\_app\_id

177a7e61-c000-0001-0000-000000000003

primary\_siem\_app\_id

177a7e61-c000-0001-0000-000000000003

storage\_app\_name

MaxPatrol 10

storage\_app\_alias

MP-1

storage\_app\_id

1ab005a0-9100-0001-0000-000000000004

Collection point

Рисунок 7 - третий фильтр

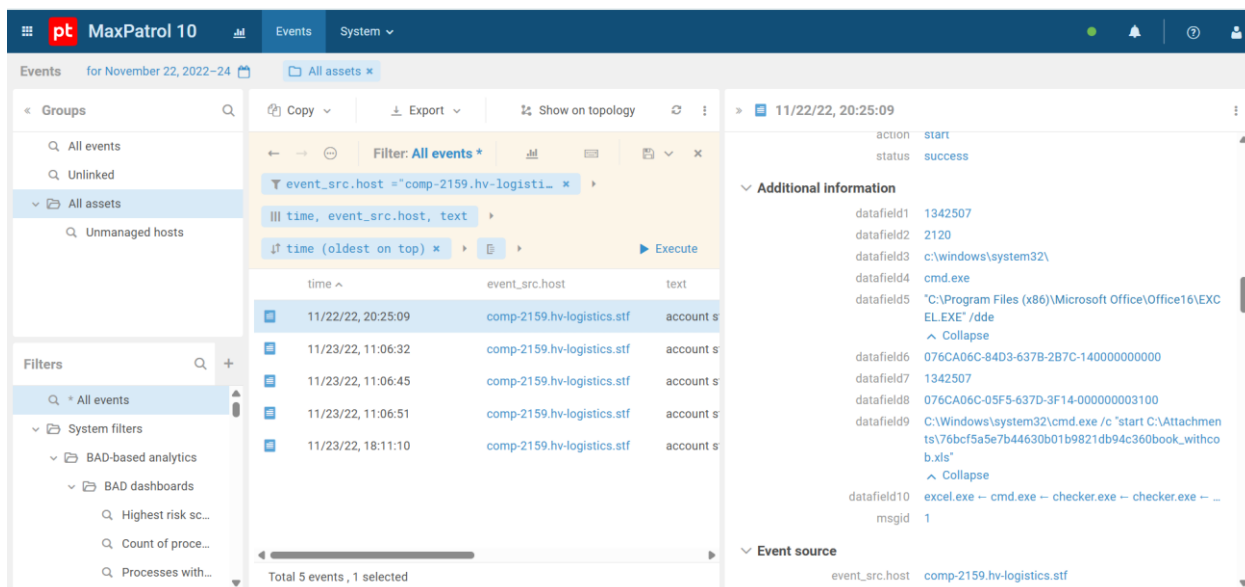


Рисунок 8 - найденный файл

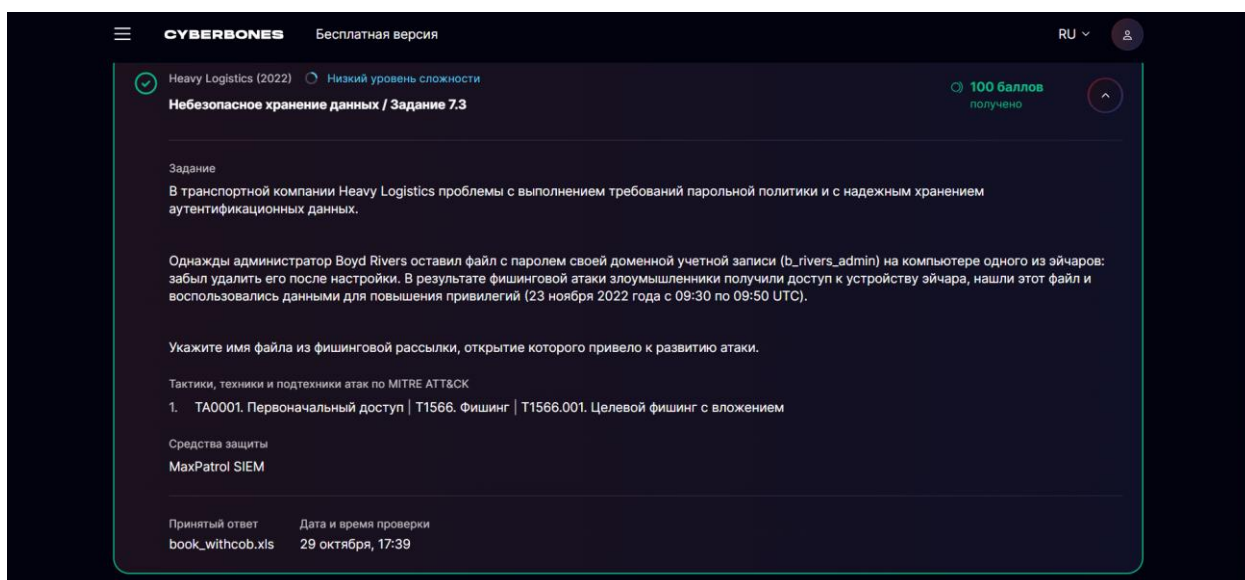


Рисунок 9 - третий ответ