EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

Správa a dohled nad počítačovou sítí

SOC – Vytvoření a smazání účtu během 24 hodin

Metodický list

Autor: Ing. Josef Bezchleba, Metodik: Bc. Jaroslav Tihlařík

Recenzent: Ing. Peter Jankovský

Rok vydání: 2023

Obsah

Cíle

- Žák vlastními slovy popíše možné problémy spojené s aktivitou vytváření a mazání uživatelských účtů během krátkého časového období (např. během 24 hodin).

Dovednosti

- Žák navrhne a aplikuje filtr pro vyhledání záznamů v ArcSight Loggeru související s vytvořením a/nebo smazáním uživatelských účtů.
- Žák interpretuje výsledky vyhledávání.
- Žák identifikuje účty, které byly vytvořeny a/nebo smazány během 24 hodin.
- Žák navrhne a aplikuje filtr a pravidla pro automatické vyhodnocování událostí v nástroji ArcSight ESM.

Pracovní prostředí

Úlohu lze realizovat v prostředí Cylab JCEKB

Pro práci budeme potřebovat následující:

- SCx[1] Replay Connector
- ArcSight Logger
- ArcSight ESM
- Dokument ArcSight Categorization.xlsx
- Dokument ArcSight CommonEventFormatV25.pdf

[1] Za x dosaťte číslo SC, které vám bylo přiřazeno administrátorem Cylabu.

1 Průběh výuky

Přihlaste se v prostředí Cylab do Replay Connectoru.

1. Opakování z předchozí hodiny
2. Spusťte program *ArcSight Replay Connector* (zástupce na ploše)
3. Přejděte na kartu *Replay*
4. Před spuštěním provozu nastavte následující parametry
    a. Část Logger: 100 událostí za **minutu**
    b. Část ESM: 100 událostí za **minutu**
5. Spusťte následující provoz a nechte jej běžet – POZOR platí pouze pro Logger :
    a. dhcp_3h.events
    b. dns_3h.events
    c. winc_3h.events
    d. UC3_User-Account/add_user.events
    e. UC3_User-Account/del_user.events
6. Spusťte následující provoz a nechte jej běžet – POZOR platí pouze pro ESM:
    a. dhcp_3h.events
    b. dns_3h.events
    c. winc_3h.events

    pozn. Ostatní události se budou zapínat postupně při tvorbě pravidla.

2 Zadání

2.1 ČÁST Logger

1. Jaké uživatelské účty byly vytvořeny během posledních 24 hodin?
   - Postup:
     - Hledáme události vytvoření uživatelského účtu.
     - Dotaz + funkce „top“ nebo „chart“
     - CEF pole
       - *categoryBehavior* | *externalId* | *deviceEventClassId*
         - | = OR –> je možné použít jedno z uvedených
       - *destinationUserName* = název vytvořeného účtu
     - Microsoft Windows -> 4720: A user account was created

   - Dotaz:

```
categoryBehavior = "/Authentication/Add" | top destinationUserName
```

   - Správná odpověď: **ceastwood, dhoffman, jdepp, jlopez, sstalone**

2. Který uživatel vytvořil tyto účty?
   - Postup:
     - Hledáme události vytvoření uživatelského účtu.
       - Microsoft Windows -> 4720: A user account was created
     - Dotaz + funkce „top“ nebo „chart“
     - CEF pole
       - *categoryBehavior* | *externalId* | *deviceEventClassId*
       - *destinationUserName* = název vytvořeného účtu
       - *sourceUserName* = název uživatele který účet vytvářel

   - Dotaz:

```
categoryBehavior = "/Authentication/Add" | top destinationUserName, sourceUserName
```

   - Správná odpověď: **Administrator**

3. Na jakém serveru byly účty vytvořeny?
   - Postup:
     - Hledáme události vytvoření uživatelského účtu.
       - Microsoft Windows -> 4720: A user account was created
     - Dotaz + funkce „top“ nebo „chart“
     - CEF pole
       - *categoryBehavior* | *externalId* | *deviceEventClassId*
       - *destinationUserName* = název vytvořeného účtu
       - *sourceUserName* = název uživatele který účet vytvářel
       - *destinationHostName* = na jakém serveru

   - Dotaz:

```
categoryBehavior = "/Authentication/Add" | top destinationHostName, sourceUserName,
destinationHostName
```

   - Správná odpověď: **dc1.cylab.lan**

Pokročilejší:

4. Zjisti, jestli byl nějaký uživatelský účet smazán během posledních 24 hodin.
   - Postup:
     - Hledáme události smazání uživatelského účtu.
       - Microsoft Windows -> 4726: A user account was deleted
     - Dotaz + funkce „top“ nebo „chart“
     - CEF pole
       - *categoryBehavior* | *externalId* | *deviceEventClassId*
       - *sourceUserName* = název uživatele který smazal účty
       - *destinationUserName* = jaké účty byly smazány
       - *destinationHostName* = na jakém serveru
   - Dotaz:

```
categoryBehavior = "/Authentication/Delete" | top sourceUserName, destinationUserName,
destinationHostName
```

   - Správná odpověď: **jdepp, ceastwood**

5. Vyšetři, jestli některý z účtů neprováděl aktivitu Brute-Force Login.
   - Postup:
     - Hledáme události neúspěšného přihlášení uživatele.
       - Microsoft Windows -> 4625: An account failed to log on
     - Dotaz + funkce „top“ nebo „chart“
     - CEF pole
       - *categoryBehavior* | *externalId* | *deviceEventClassId*
       - *destinationUserName* = název uživatele
   - Dotaz:

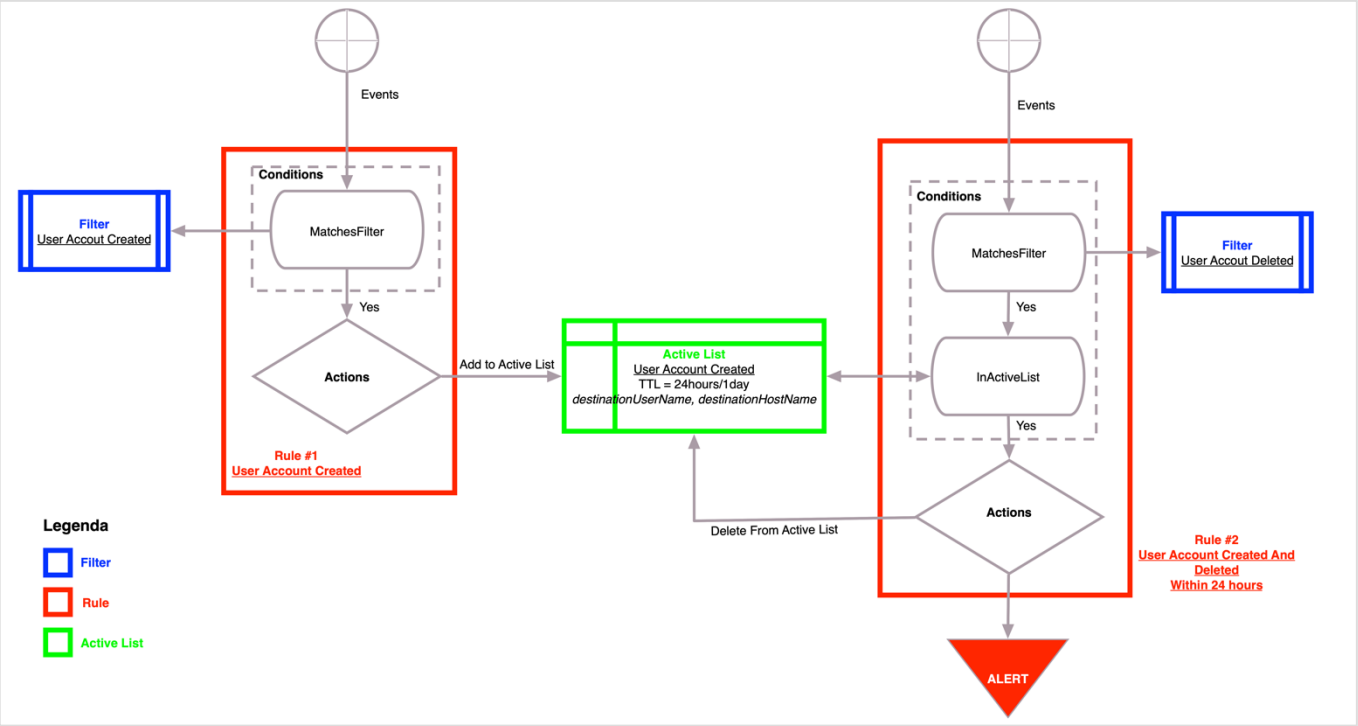
```
CategoryBehavior = /Authentication/Verify AND categoryOutcome = /Failure | top
destinationUserName
```

     - Správná odpověď: **Žádný účet aktivitu Brute-Force Login neprováděl.**

2.2 ČÁST ESM

1. Vytvořte pravidlo, které bude detekovat v reálném čase vytvoření a smazání uživatelského účtu během 24 hodin.

2.2.1 Schéma pravidla



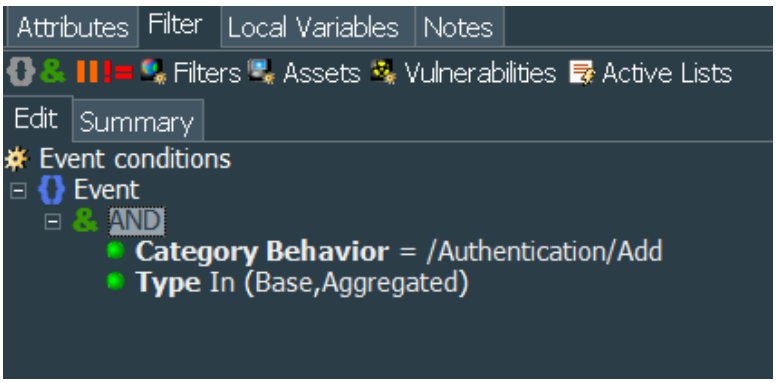
2.2.2 Postup tvorby pravidla

1. Vytvořit Filtr #1 – User Account Created (samostatně)
    a. Učitel spustí provoz - **UC3_User-Account/add_user.events**
    b. Funkčnost filtru ověříme pomocí Active Channel.
2. Vytvořit Active List #1 – User Account Created (s učitelem)
3. Vytvořit Rule #1 – User Account Created (s učitelem)
    a. Aktivujeme pravidlo.
    b. Ověříme, že se na Active Listu vytvořily záznamy o vytvořených uživatelích.
4. Vytvořit Filtr #2 – User Account Deleted (samostatně)
    a. Učitel zastaví provoz - **UC3_User-Account/add_user.events**
    b. Učitel spustí provoz - **UC3_User-Account/del_user.events**
    c. Funkčnost filtru ověříme přes Active Channel.
5. Vytvořit Rule #2 – User Account Created And Deleted Within 24 Hours (s učitelem)
    a. Aktivujeme pravidlo.
    b. Ověříme pomocí Active Channel vznik alertů.
    c. Ověříme, že se smazaly záznamy smazaných uživatelů z Active Listu.
6. Úklid ESM.

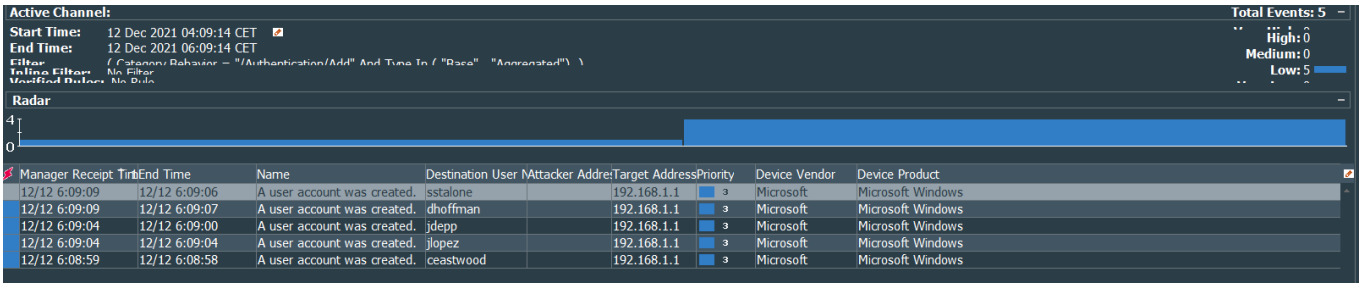
Návod:

2.2.3 Filtr #1 – User Account Created

1. Vytvoříme nový filtr *Filters -> SC[x]'s Filters -> KB[x] [Prijmeni] -> UC3_[Prijmeni]_User_Account_Created*

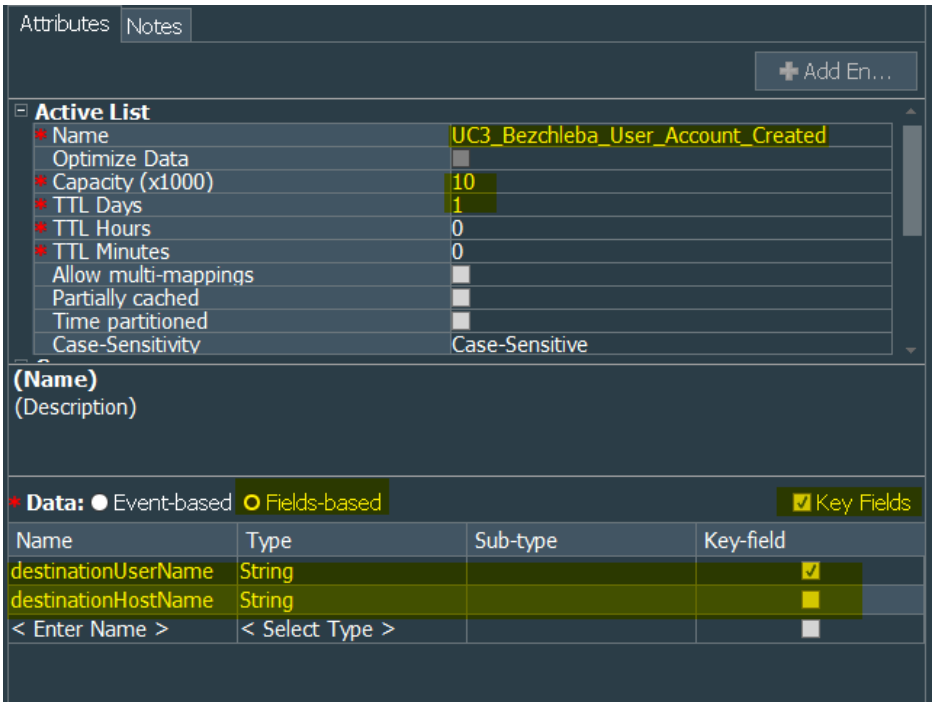


Pomocí Active Channel ověříme funkčnost filtru:



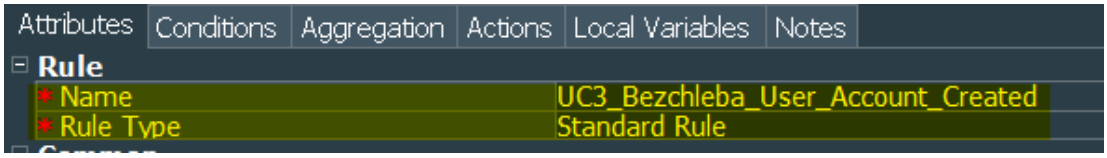
2.2.4 Active List #1 – User Account Created

1. Vytvoříme nový Active List *Lists -> Active Lists -> SC[x]'s Active Lists -> KB[x] [Prijmeni] -> UC3_[Prijmeni]_User_Account_Created*

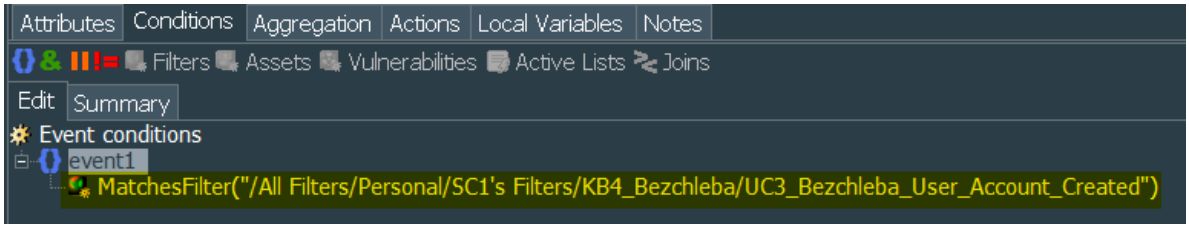


2.2.5 Rule #1 – User Account Created

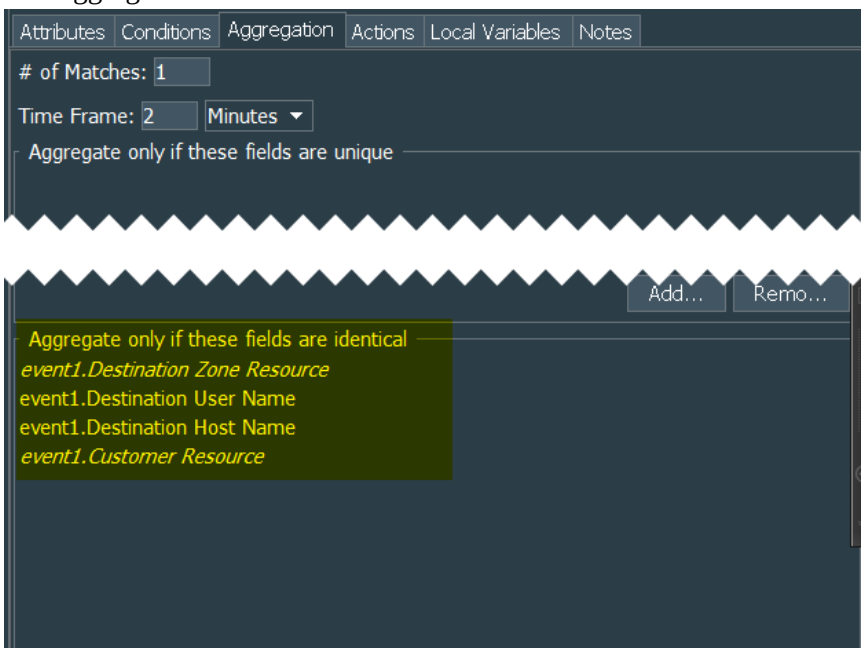
1. Vytvoříme pravidlo Rules -> *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC3_[Prijmeni]_User_Account_Created*
   a. Attributes



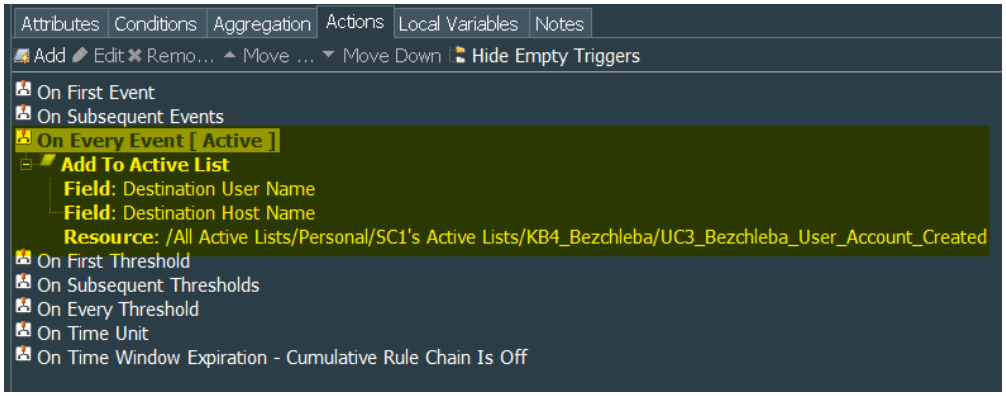
   b. Conditions



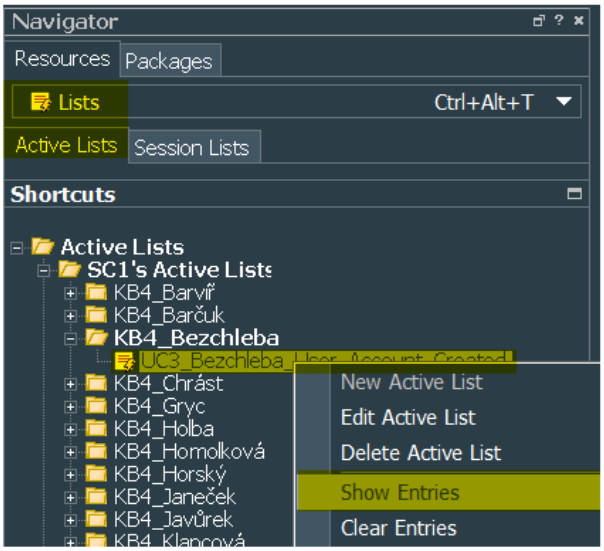
   c. Aggregation



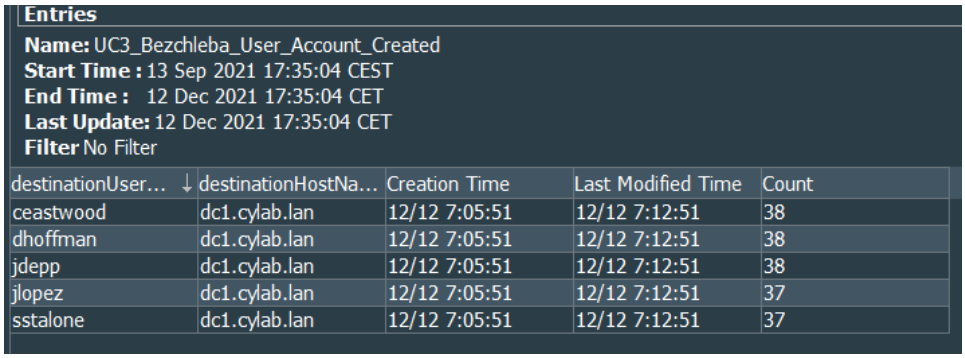
   d. Actions



2. Pravidlo přesuneme metodou „Drag & Drop“ do složky *Rules -> Shared -> SC[x] Real-Time Rules*
    a. **Ve vyskakovacím okně „Drag & Drop zvolím Link.**
3. Pravidlo je aktivní a začíná korelovat.
4. Správnou funkčnost pravidla ověříme tak, že si zobrazíme obsah Active Listu *UC3_[Prijmeni]_User_Account_Created*.



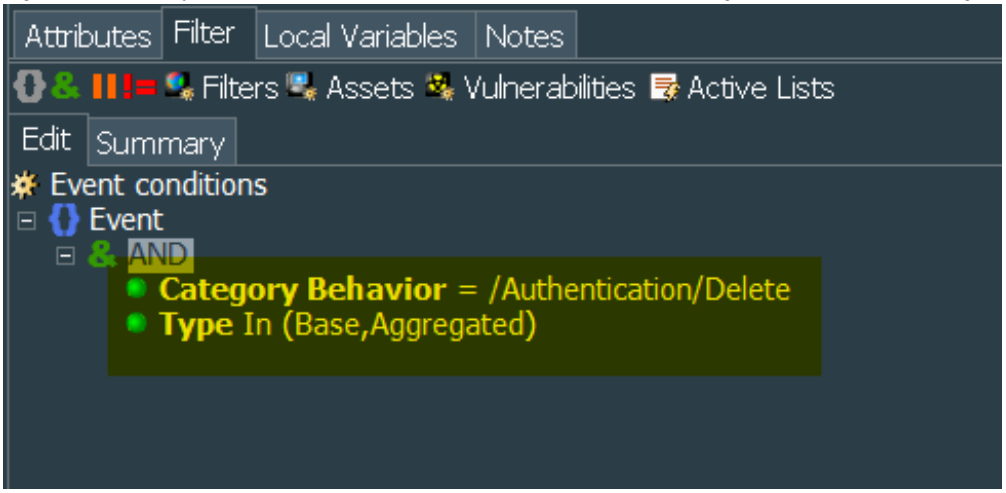
List by měl obsahovat seznam vytvořených účtů.



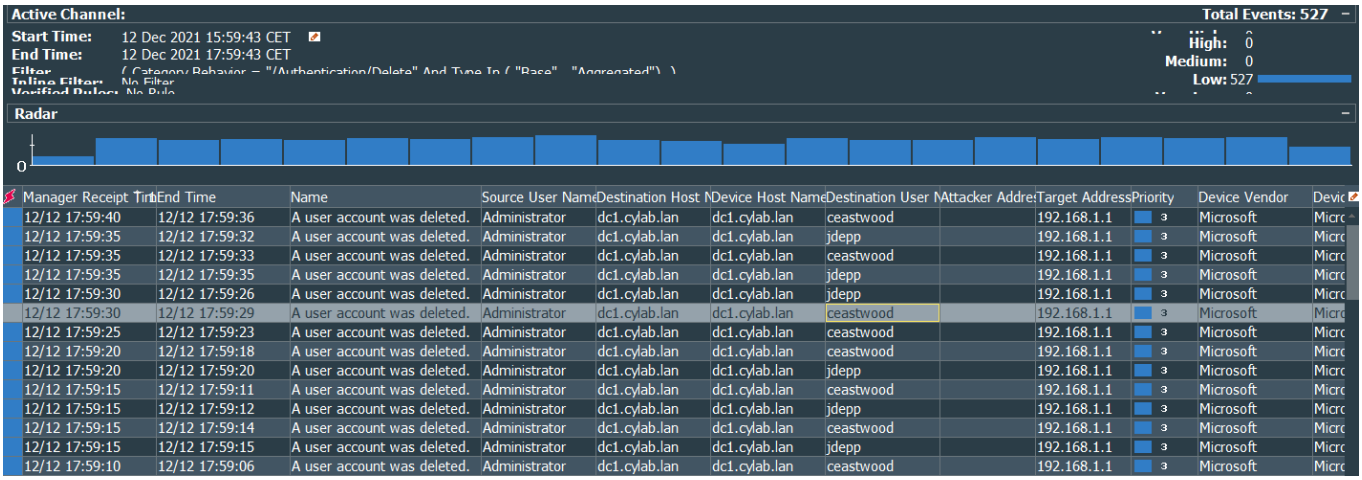
destinationUser...	destinationHostNa...	Creation Time	Last Modified Time	Count
ceastwood	dc1.cylab.lan	12/12 7:05:51	12/12 7:12:51	38
dhoffman	dc1.cylab.lan	12/12 7:05:51	12/12 7:12:51	38
jdepp	dc1.cylab.lan	12/12 7:05:51	12/12 7:12:51	38
jlopez	dc1.cylab.lan	12/12 7:05:51	12/12 7:12:51	37
sstalone	dc1.cylab.lan	12/12 7:05:51	12/12 7:12:51	37

2.2.6 Filtr #2 – User Account Deleted

1. Vytvoříme nový filtr *Filters -> SC[x]’s Filters -> KB[x] [Prijmeni] -> UC3_[Prijmeni]_User_Account_Deleted*

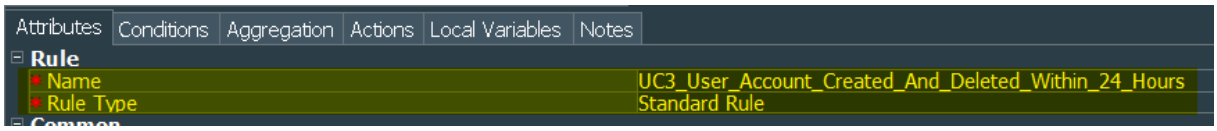


Pomocí Active Channel ověříme funkčnost filtru:

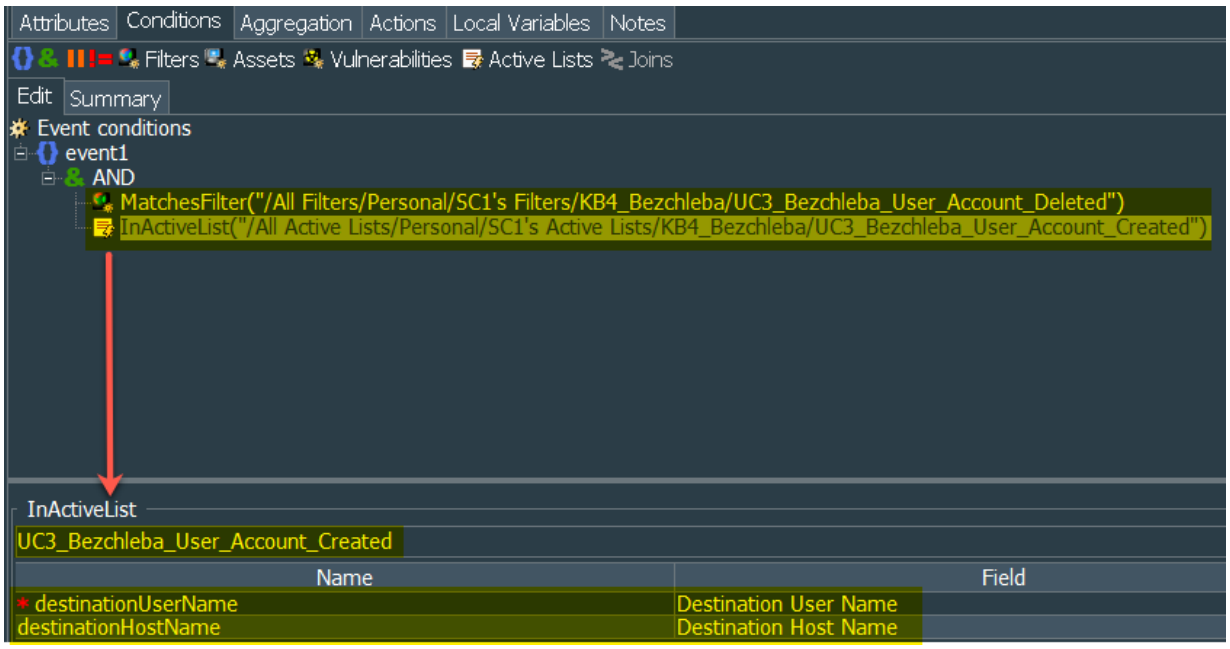


2.2.7 Rule #2 – User Account Created And Deleted Within 24 Hours

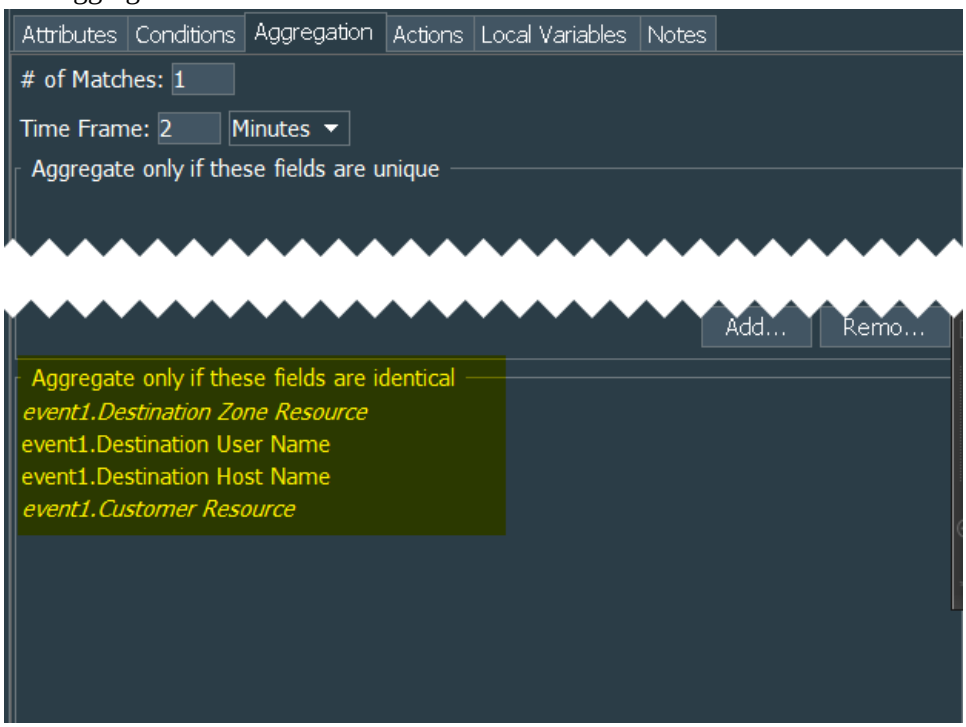
1. Vytvoříme pravidlo Rules -> *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC3_[Prijmeni]_User_Account_Created_And_Deleted_Within_24_Hours*
   a. Attributes



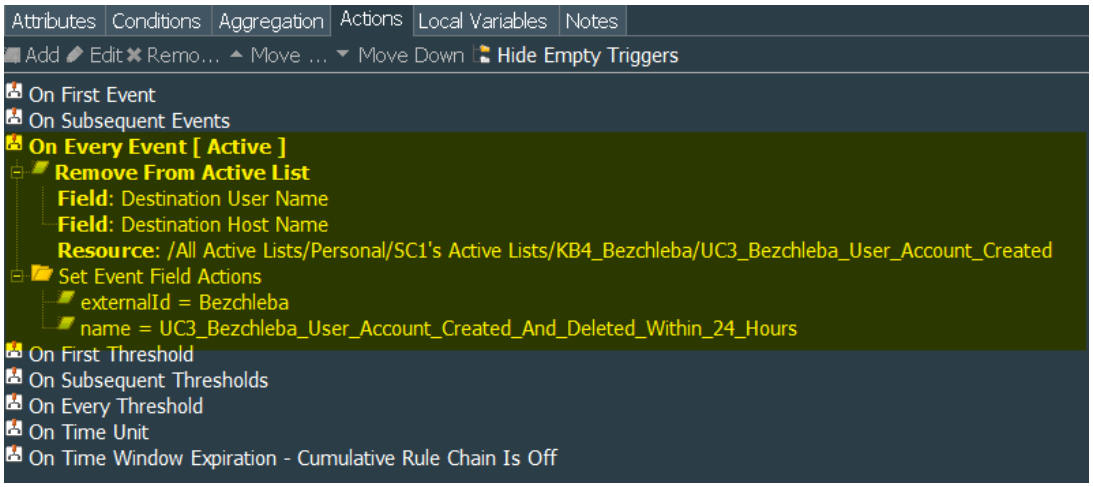
   b. Conditions



c. Aggregation



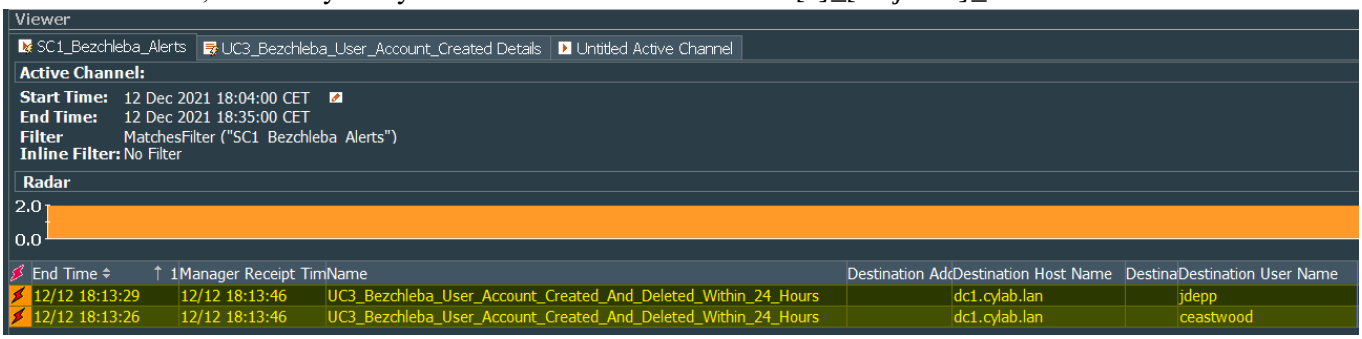
d. Actions



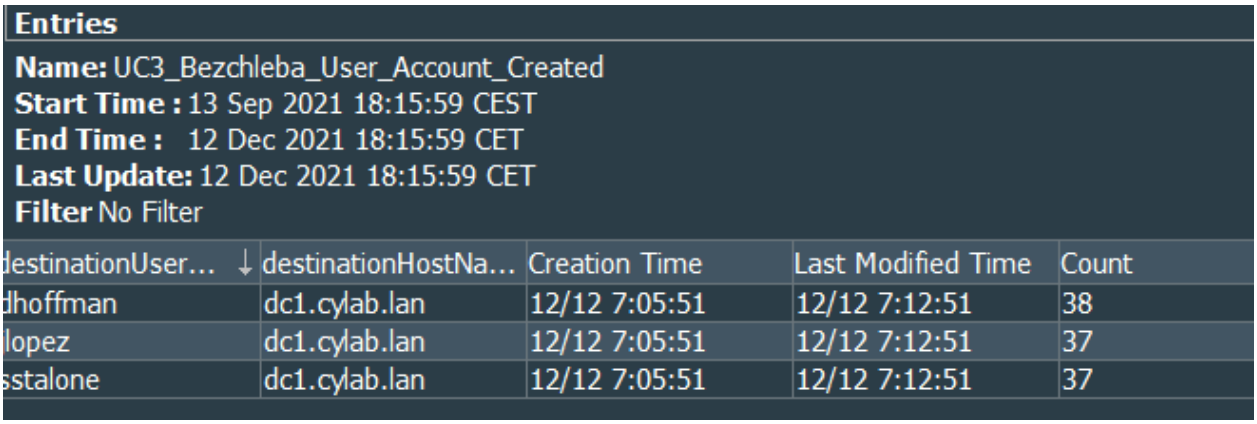
2. Pravidlo přesuneme metodou „Drag & Drop“ do složky *Rules -> Shared -> SC[x] Real-Time Rules*
   a. **Ve vyskakovacím okně „Drag & Drop zvolím Link.**
3. Pravidlo je aktivní a začíná korelovat.

2.2.8 Ověření funkčnosti pravidla

1. Ověříme, že vznikly alerty – zobrazíme Active Channel *SC[x]_[Prijmeni]_Alerts.*

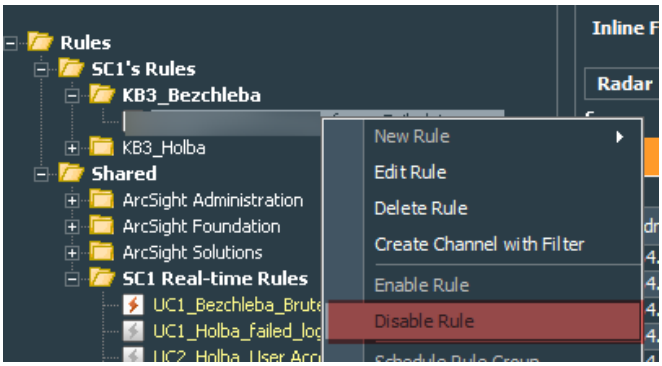


2. Ověříme, že se z Active Listu *UC3_[Prijmeni]_User_Account_Created* smazaly záznamy o uživatelských účtech na které alert vznikl.

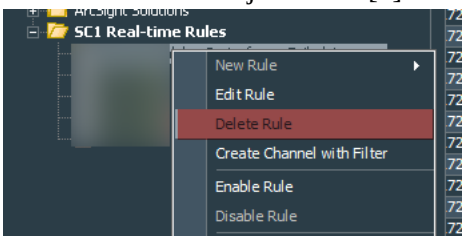


2.2.9 Úklid ESM

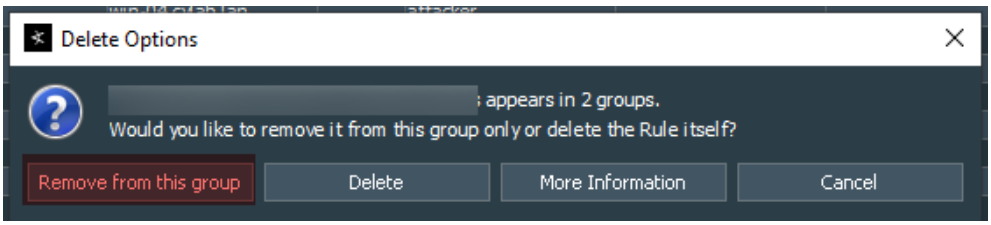
1. Vypneme pravidla:
   a. *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC3_[Prijmeni]_User_Account_Created*
   b. *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC3_[Prijmeni]_User_Account_Created_And_Deleted_Within_24_Hours*



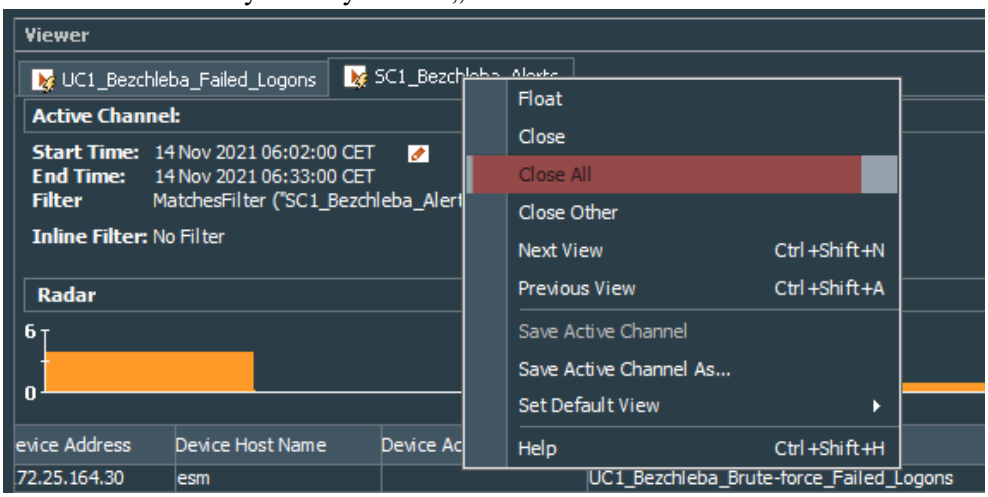
2. Pravidlo odlinkujeme z SC[x] Real-time Rules.



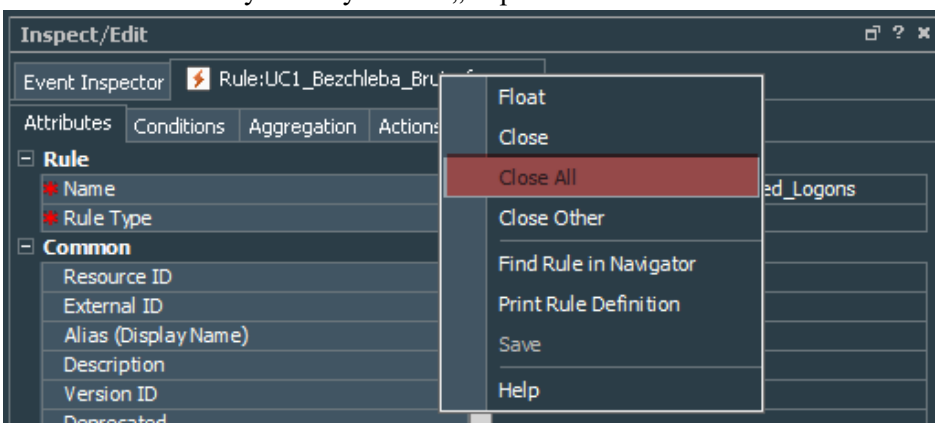
Pozor!!! Zvolíme – „Remove from this group“. Pokud bychom zvolil možnost „Delete“, tak pravidlo se celé smaže.



3. Zavřeme všechny záložky v okně „Viewer“.



4. Zavřeme všechny záložky v okně „Inspect/Edit“



Seznam použitých zdrojů

Windows Security Log Event ID 4625. *Ultimate IT Security* [online]. [cit. 2021-12-16]. Dostupné z: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

Brute Force. *MITRE ATT&CK* [online]. [cit. 2021-12-16]. Dostupné z: https://attack.mitre.org/techniques/T1110/