



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



jihořmoravský kraj

Správa a dohled nad počítačovou sítí

SOC – Vytvoření a smazání účtu během 24 hodin

Metodický list

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

Recenzent: Ing. Peter Jankovský

Rok vydání: 2023

SOC - Vytvoření a smazání účtu během 24 hodin podléhá licenci CC BY-SA 4.0 International License (Offline use:
<http://creativecommons.org/licenses/by-nc-sa/4.0/>).



Obsah

| | |
|---|----|
| Cíle..... | 2 |
| Dovednosti | 2 |
| Pracovní prostředí | 2 |
| 1 Průběh výuky..... | 3 |
| 2 Zadání..... | 4 |
| 2.1 ČÁST Logger..... | 4 |
| 2.2 ČÁST ESM | 6 |
| 2.2.1 Schéma pravidla..... | 6 |
| 2.2.2 Postup tvorby pravidla | 6 |
| Návod:..... | 7 |
| 2.2.3 Filtr #1 – User Account Created | 7 |
| 2.2.4 Active List #1 – User Account Created | 7 |
| 2.2.5 Rule #1 – User Account Created..... | 8 |
| 2.2.6 Filtr #2 – User Account Deleted | 9 |
| 2.2.7 Rule #2 – User Account Created And Deleted Within 24 Hours..... | 10 |
| 2.2.8 Ověření funkčnosti pravidla..... | 12 |
| 2.2.9 Úklid ESM | 12 |
| Seznam použitých zdrojů..... | 14 |

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:

- SCx¹ Replay Connector
- ArcSight Logger
- ArcSight ESM
- Dokument ArcSight Categorization.xlsx
- Dokument ArcSight CommonEventFormatV25.pdf

¹ Za x dosaďte 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. Zjistí, 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. Vyšetří, 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:

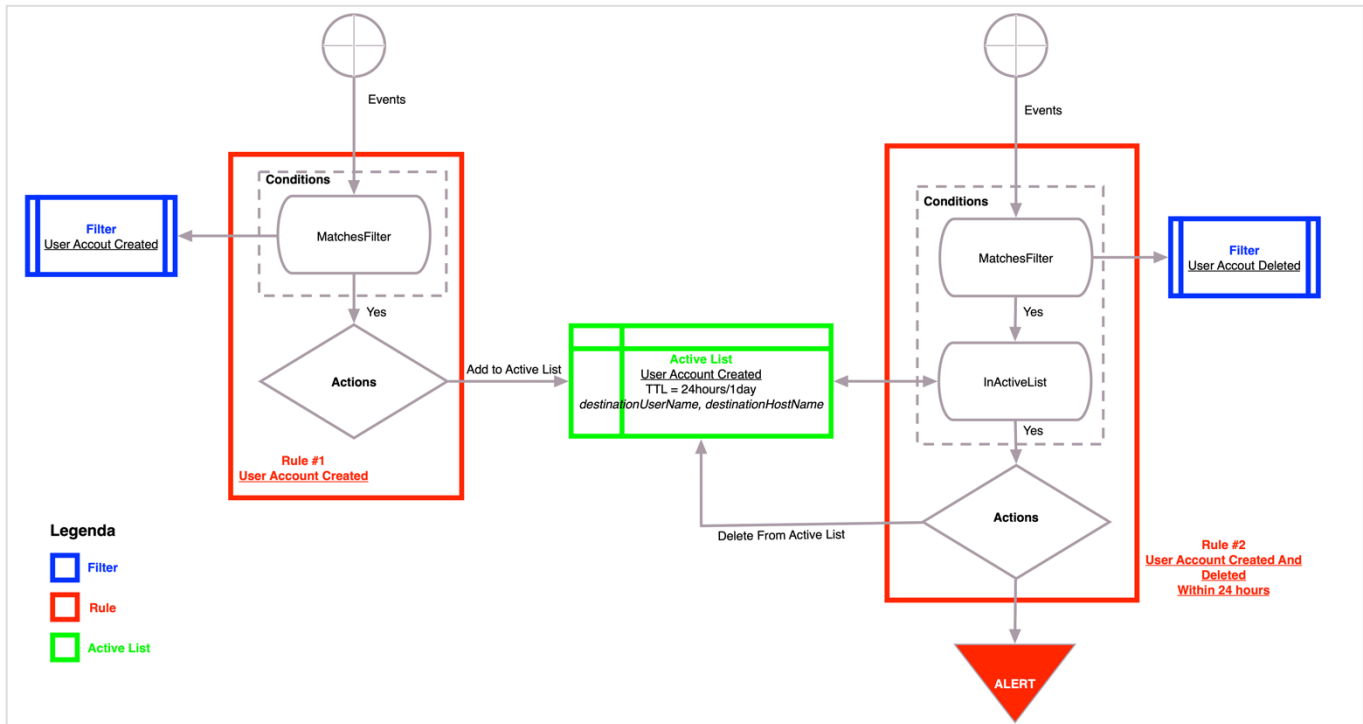
```
CategoryBehavior = /Authentication/Verify AND categoryOutcome = /Failure | top destinationUserName
```

- 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



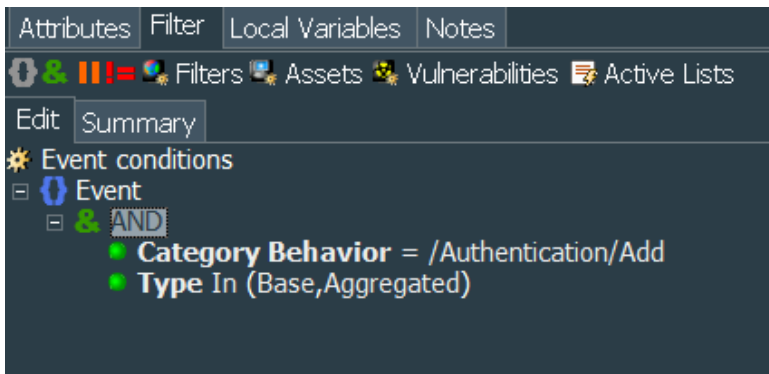
2.2.2 Postup tvorby pravidla

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 uživateli.
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.

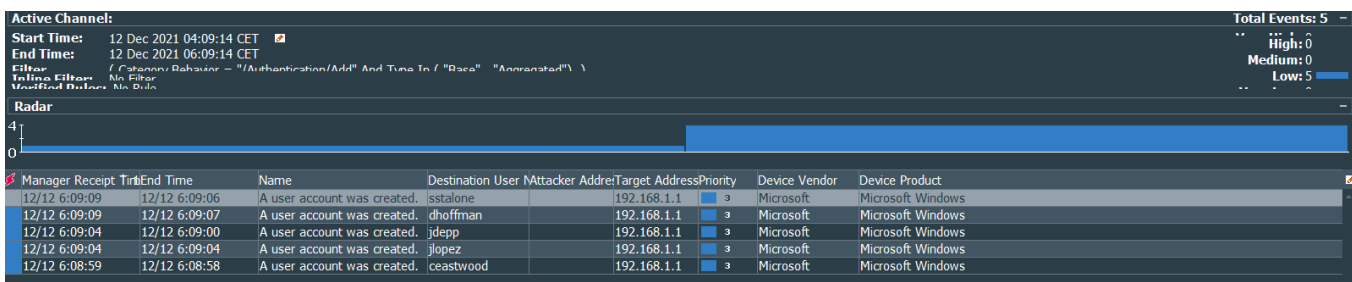
Návod:

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*

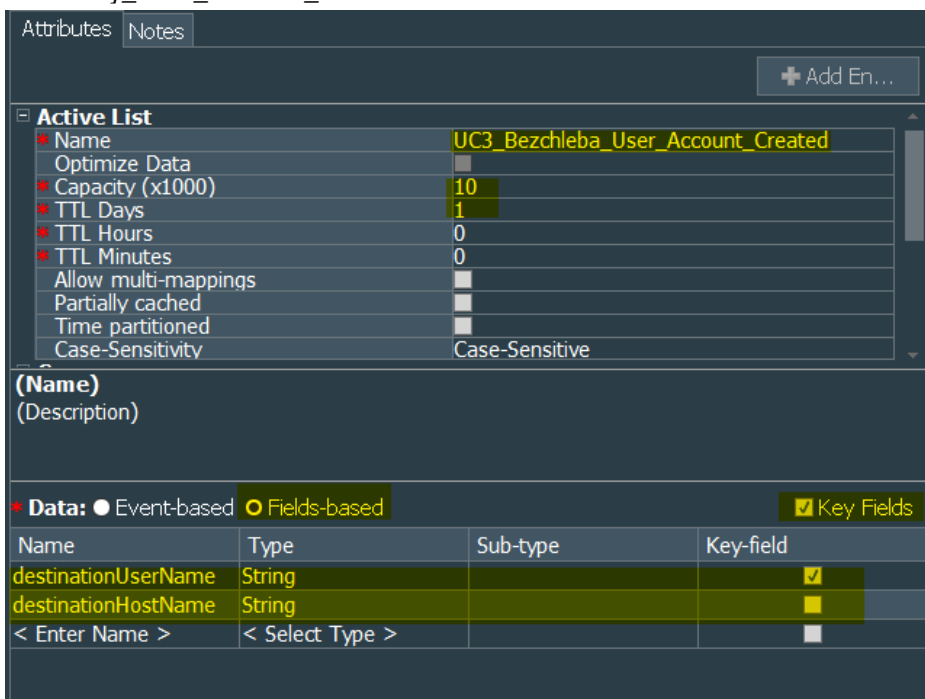


Pomocí Active Channel ověříme funkčnost filtru:



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

The screenshot shows the 'Attributes' tab of a rule configuration interface. The rule name is 'UC3_Bezchleba_User_Account_Created' and the rule type is 'Standard Rule'.

| Attribute | Value |
|-----------|------------------------------------|
| Name | UC3_Bezchleba_User_Account_Created |
| Rule Type | Standard Rule |

b. Conditions

The screenshot shows the 'Conditions' tab. An event condition named 'event1' is defined with the following filter:

```
MatchesFilter("/All Filters/Personal/SC1's Filters/KB4_Bezchleba/UC3_Bezchleba_User_Account_Created")
```

c. Aggregation

The screenshot shows the 'Aggregation' tab. The configuration includes:

- # of Matches: 1
- Time Frame: 2 Minutes
- Aggregate only if these fields are unique

Fields to aggregate on (if identical):

- event1.Destination Zone Resource
- event1.Destination User Name
- event1.Destination Host Name
- event1.Customer Resource

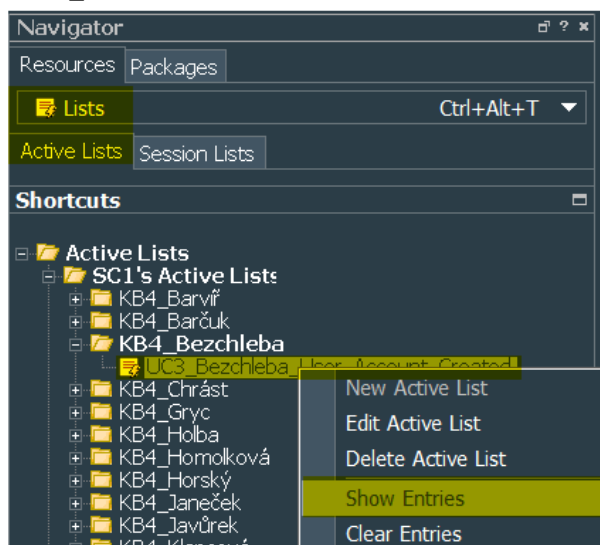
d. Actions

The screenshot shows the 'Actions' tab. The selected action is 'On Every Event [Active]', which includes:

- Add To Active List
 - Field: Destination User Name
 - Field: Destination Host Name
 - Resource: /All Active Lists/Personal/SC1's Active Lists/KB4_Bezchleba/UC3_Bezchleba_User_Account_Created

Other available actions include: On First Event, On Subsequent Events, On First Threshold, On Subsequent Thresholds, On Every Threshold, On Time Unit, and On Time Window Expiration - Cumulative Rule Chain Is Off.

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*.

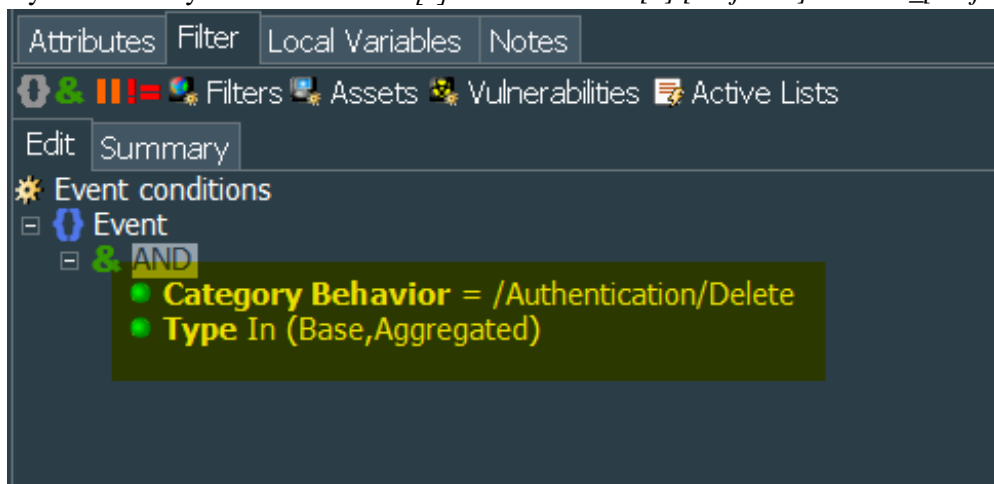


List by měl obsahovat seznam vytvořených účtů.

| Entries | | | | | |
|---|----------------------|---------------|--------------------|-------|--|
| Name: UC3_Bezchleba_User_Account_Created | | | | | |
| Start Time : 13 Sep 2021 17:35:04 CEST | | | | | |
| End Time : 12 Dec 2021 17:35:04 CET | | | | | |
| Last Update: 12 Dec 2021 17:35:04 CET | | | | | |
| Filter No Filter | | | | | |
| 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:

Active Channel: Total Events: 527

Start Time: 12 Dec 2021 15:59:43 CET
 End Time: 12 Dec 2021 17:59:43 CET
 Filter: (Category Behavior - "/Authentication/Deletes" And Time In ("Base" "Annotated"))
 In-Line Filter: No Filter
 Verified Rules: No Rule

High: 0
 Medium: 0
 Low: 527

Radar

| Time | End Time | Name | Source User Name | Destination Host | Device Host Name | Destination User | Attacker Address | Target Address | Priority | Device Vendor | Device |
|----------------|----------------|-----------------------------|------------------|------------------|------------------|------------------|------------------|----------------|----------|---------------|--------|
| 12/12 17:59:40 | 12/12 17:59:36 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:35 | 12/12 17:59:32 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | jdepp | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:35 | 12/12 17:59:33 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:35 | 12/12 17:59:35 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | jdepp | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:30 | 12/12 17:59:26 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | jdepp | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:30 | 12/12 17:59:29 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:25 | 12/12 17:59:23 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:20 | 12/12 17:59:18 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:20 | 12/12 17:59:20 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | jdepp | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:15 | 12/12 17:59:11 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:15 | 12/12 17:59:12 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | jdepp | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:15 | 12/12 17:59:14 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:15 | 12/12 17:59:15 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | jdepp | | 192.168.1.1 | 3 | Microsoft | Micrc |
| 12/12 17:59:10 | 12/12 17:59:06 | A user account was deleted. | Administrator | dc1.cylab.lan | dc1.cylab.lan | ceastwood | | 192.168.1.1 | 3 | Microsoft | Micrc |

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

Attributes | Conditions | Aggregation | Actions | Local Variables | Notes

Rule

- Name: UC3_User_Account_Created_And_Deleted_Within_24_Hours
- Rule Type: Standard Rule

b. Conditions

Attributes | Conditions | Aggregation | Actions | Local Variables | Notes

Filters | Assets | Vulnerabilities | Active Lists | Joins

Edit | Summary

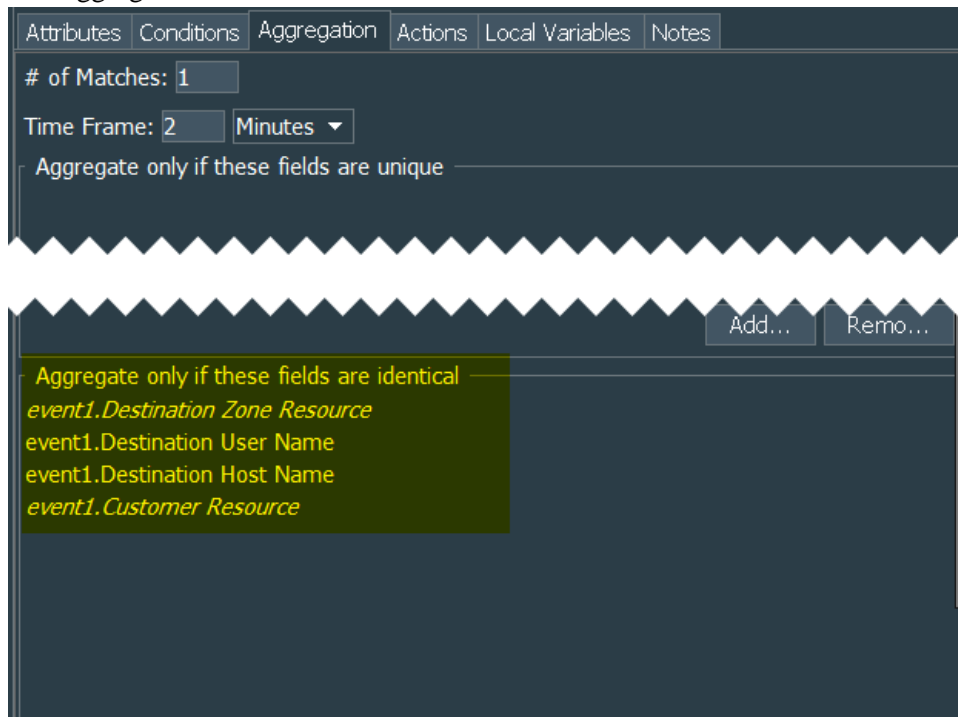
Event conditions

- event1
 - AND
 - MatchesFilter("/All Filters/Personal/SC1's Filters/KB4_Bezchleba/UC3_Bezchleba_User_Account_Deleted")
 - InActiveList("/All Active Lists/Personal/SC1's Active Lists/KB4_Bezchleba/UC3_Bezchleba_User_Account_Created")

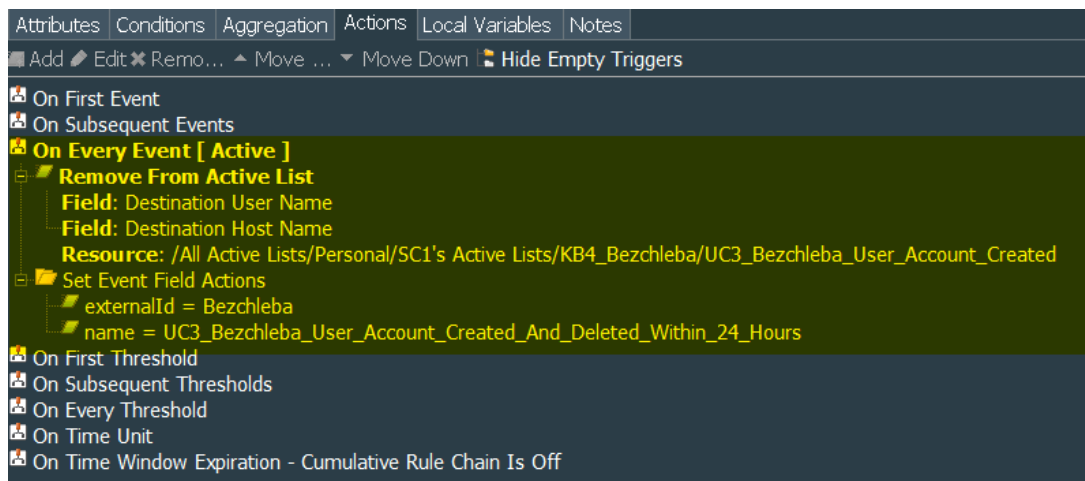
InActiveList

| UC3_Bezchleba_User_Account_Created | |
|------------------------------------|-----------------------|
| Name | Field |
| * destinationUserName | Destination User Name |
| destinationHostName | Destination Host Name |

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*.

| End Time | Manager Receipt Time | TimName | Destination | Host Name | User Name |
|----------------|----------------------|--|---------------|-----------|-----------|
| 12/12 18:13:29 | 12/12 18:13:46 | UC3_Bezchleba_User_Account_Created_And_Deleted_Within_24_Hours | dc1.cylab.lan | | jdepp |
| 12/12 18:13:26 | 12/12 18:13:46 | UC3_Bezchleba_User_Account_Created_And_Deleted_Within_24_Hours | dc1.cylab.lan | | ceastwood |

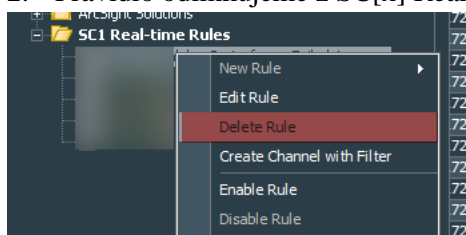
2. Ověříme, že se z Active Listu *UC3_[Prijmeni]_User_Account_Created* smazaly záznamy o uživatelských účtech na které alert vznikl.

| destinationUser... | destinationHostNa... | Creation Time | Last Modified Time | Count |
|--------------------|----------------------|---------------|--------------------|-------|
| dhoffman | dc1.cylab.lan | 12/12 7:05:51 | 12/12 7:12:51 | 38 |
| lopez | dc1.cylab.lan | 12/12 7:05:51 | 12/12 7:12:51 | 37 |
| stalone | dc1.cylab.lan | 12/12 7:05:51 | 12/12 7:12:51 | 37 |

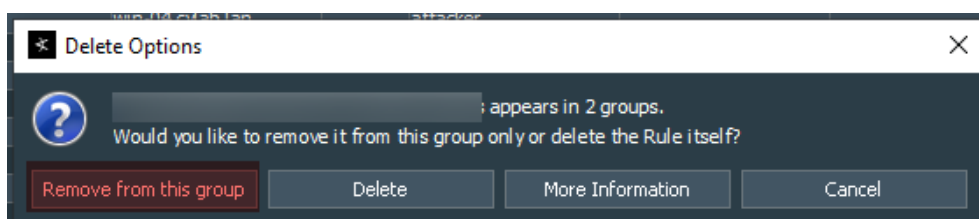
2.2.9 Úklid ESM

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

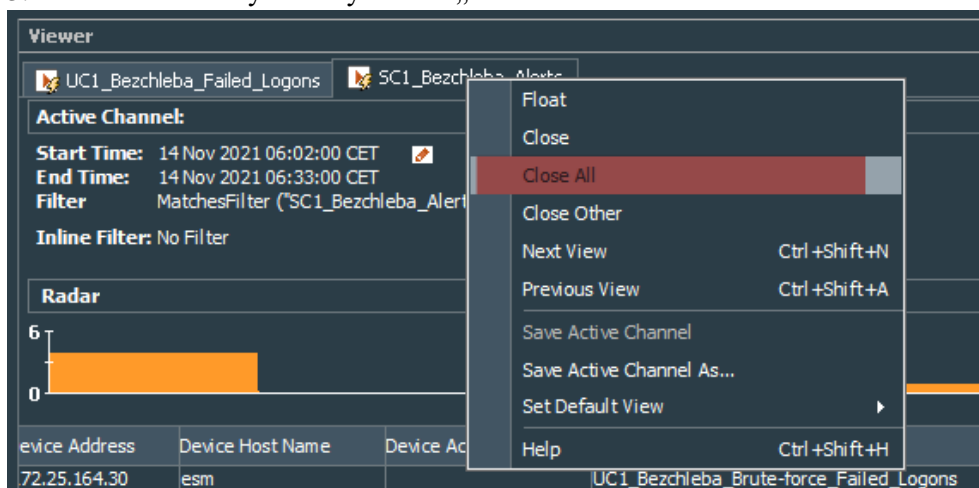
2. Pravidlo odlinkujeme z SC[x] Real-time Rules.



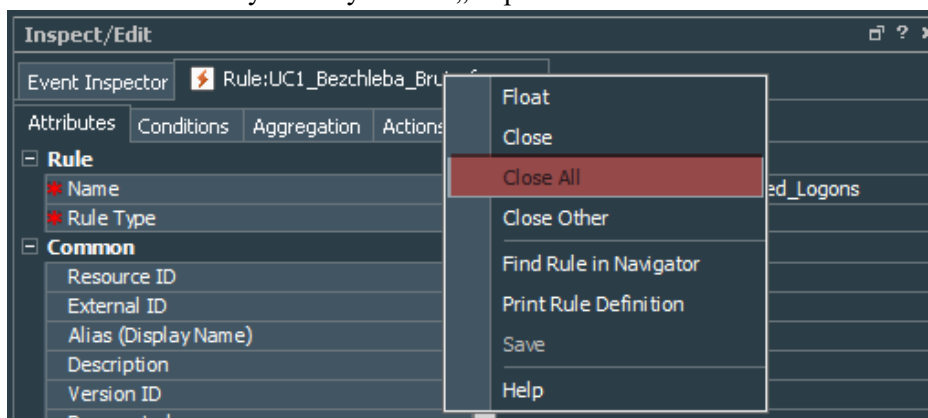
Pozor!!! Zvolíme – „Remove from this group“. Pokud bychom zvolil možnost „Delete“, tak pravidlo se celé smaže.



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/>