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 – Threat Intelligence

Metodický list

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

Recenzent: Ing. Peter Jankovský

Rok vydání: 2023

Obsah

Cíle

- Žák vlastními slovy popíše pojem Threat Intelligence.
- Žák vysvětlí přínosy využití Threat Intelligence.
- Žák vysvětlí rozdíly mezi placenými a open-source datovými zdroji.
- Žák objasní princip napojení Threat Intelligence na nástroj SIEM.

Dovednosti

- Žák navrhne a aplikuje filtr pro vyhledání záznamů v ArcSight Loggeru související s komunikací s podezřelou IP adresou, podezřelou doménou.
- Žák identifikuje zdroj, cíl a typ probíhající komunikace.
- Žák interpretuje výsledky vyhledávání.
- 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: 50 událostí za **minutu**
    b. Část ESM: 50 událostí za **minutu**
5. Spusťte následující provoz a nechte jej běžet
    a. ciscopix.recorded.events
    b. ciscovpnconcentrator.recorded.events
    c. tippingpoint.recorded.events
    d. **UC4_Threat_Intelligence.events**

2 Zadání

2.1 ČÁST Logger

1. Ověřte, zda probíhá komunikaci s podezřelou IP adresou „74.125.194.95 “?

   1.1. Pokud ano, z jakých IP adres probíhá komunikace a o jaký typ komunikace se jedná?

- Postup:
  - Hledáme události, kde se vyskytuje zdrojová nebo cílová adresa.
    - Typicky tyto události logují zařízení typu FW, Proxy, IDS/IPS, WEB servery…
  - Proč by nás měly zajímat obě adresy (cílová i zdrojová)?
    - Protože se může jednat jak o komunikaci směrem z LAN do internetu, tak také opačně z internetu směrem do LAN.
  - CEF pole
    - *sourceAddress, destinationAddress*

- Dotaz:

```
sourceAddress = "74.125.194.95" OR destinationAddress = "74.125.194.95"
destinationAddress = "74.125.194.95" | top sourceAddress, requestUrl
```

- Správná odpověď: **Na podezřelou cílovou IP adresu 74.125.194.95 byla zaznamenána komunikace ze tří zdrojových IP adres. Jedná se o komunikaci typu HTTP/HTTPS.**

sourceAddress	requestUrl
10.93.62.83	http://imasdk.googleapis.com:80/flash/sdkloader /vpaid1adsdk.swf?adTagUrl=http%253A%252F%252Fgoogleads.g.doubleclick.net%25... video-pub-5572812818232555%2526slotname%253D6668286429%2526description_url%... ad_type=standardvideo&max_ad_duration=33000
10.98.32.59	tcp://maps.googleapis.com:443/
10.99.164.69	tcp://maps.googleapis.com:443/

2. Ověřte, zda probíhá komunikaci s podezřelou doménu „ovhtest.net“?

   2.1. Pokud ano, o jaký typ komunikace se jedná?

- Postup:
  - Hledáme události, kde se vyskytuje název dotčené domény.
    - Typicky tyto události logují zařízení FW, Proxy, IDS/IPS, WEB servery.
  - Proč je vhodné použít operátor CONTAINS?
    - Protože doména je součástí hostname a při použití operátoru = bychom nemuseli nic najít.
  - CEF pole
    - *destinationHostName*
    - *requestUrl*

- Dotaz:

```
destinationHostName CONTAINS "ovhtest.net" OR requestUrl CONTAINS "ovhtest.net" | top
sourceAddress, destinationHostName, transportProtocol, destinationPort
```

- Správná odpověď: **Na podezřelou doménu probíhá komunikace z jedné zdrojové IP adresy na portu UDP/53. Jedná se o komunikaci typu DNS.**

sourceAddress	destinationHostName	transportProtocol	destinationPort
10.69.4.27	ns13.ovhtest.net	UDP	53
10.69.4.27	dns106.ovhtest.net	UDP	53

3. Ověřte, zda probíhá komunikaci na podezřelou URL „tcp://api.bizographics.com:443/“?¨

- Postup
  - Hledáme události, kde se vyskytuje název dotčené URL adresy.
    - Typicky tyto události logují zařízení FW, Proxy, IDS/IPS, WEB servery.
  - Použít operátor CONTAINS
  - CEF pole
    - *requestUrl*

- Dotaz:

```
requestUrl CONTAINS tcp://api.bizographics.com:443 | top sourceAddress
```

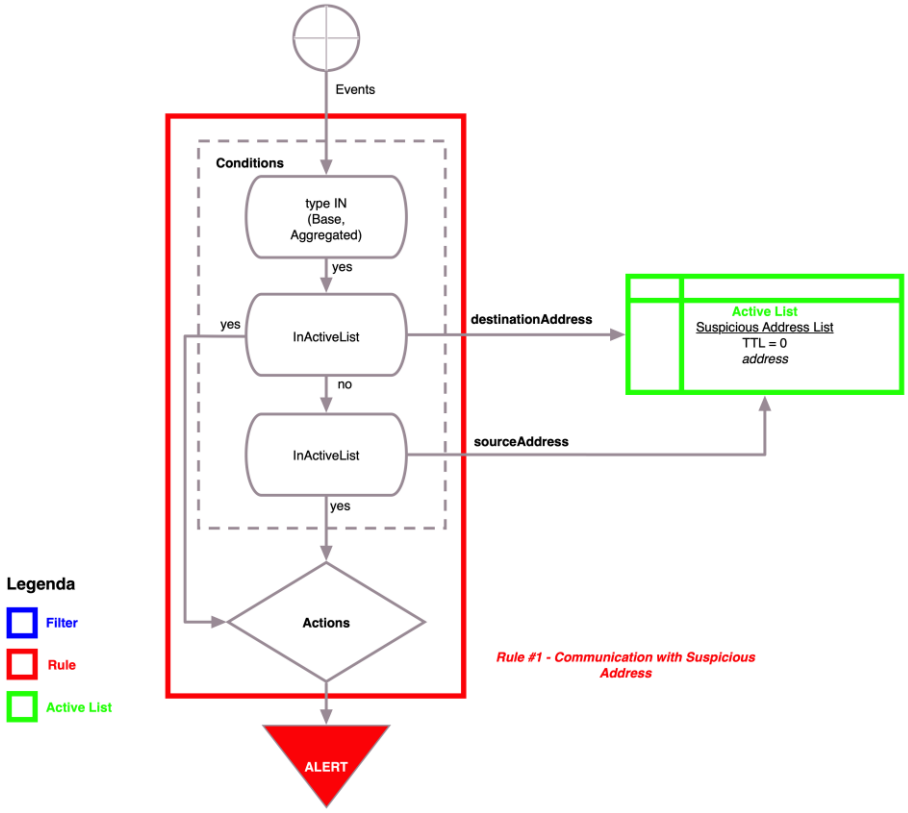
- Správná odpověď: **Na podezřelou URL probíhá komunikace z jedné zdrojové IP adresy.**

sourceAddress
10.95.153.16

2.2 ČÁST ESM

1. Vytvořte pravidlo, které bude detekovat v reálném čase pokus o komunikaci s IP adresami, které jsou uvedeny na aktivním listu „Suspicious Addresses List“.

2.2.1 Schéma pravidla



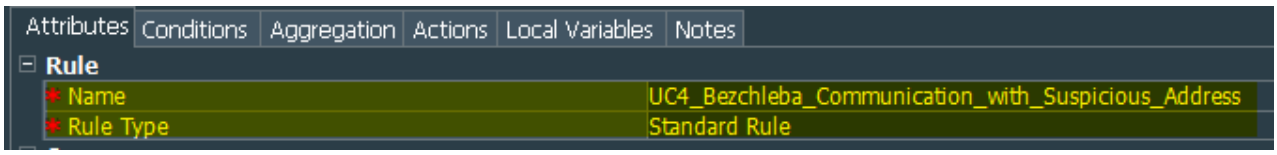
2.2.2 Postup tvorby pravidla

1. Rule #1 – Communication with Suspicious Address (samostatně)
   - Aktivujeme pravidlo.
   - Ověříme, že vznikají alerty pomocí Active Channel.
2. Úklid ESM

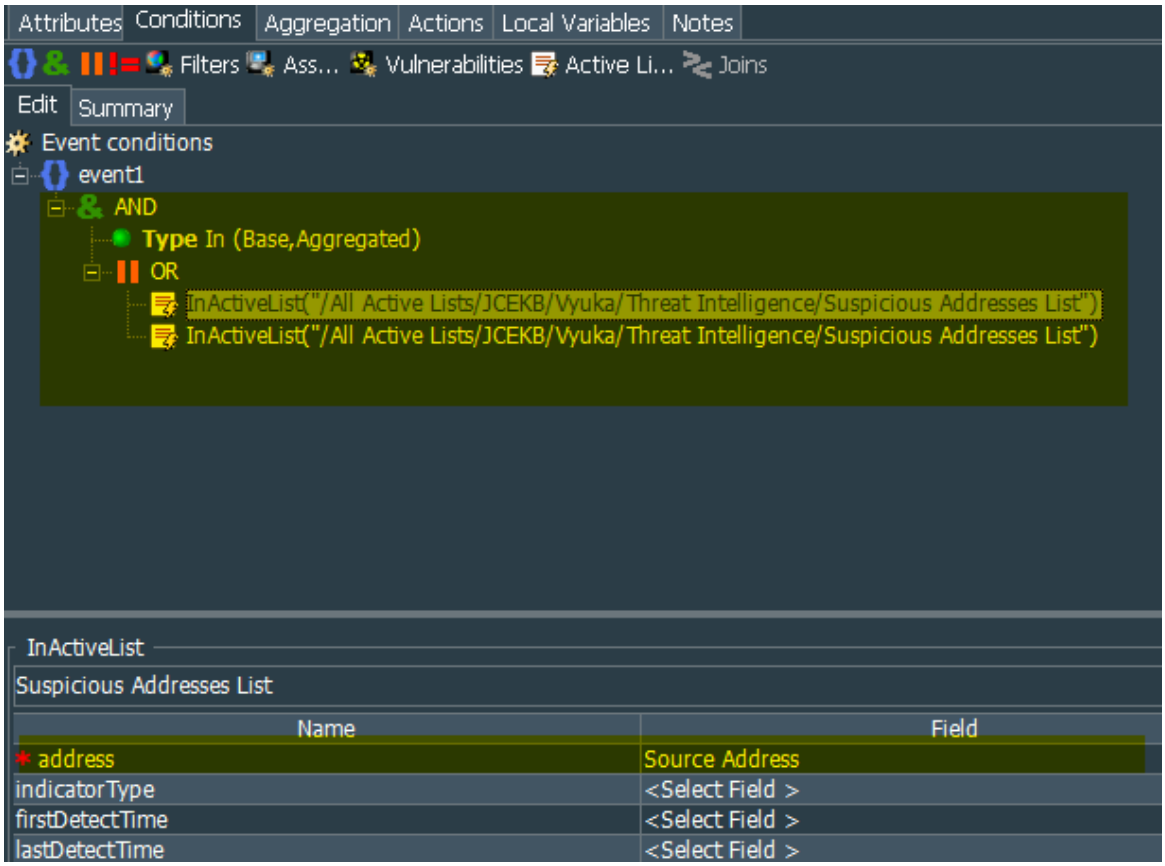
Návod:

2.2.3 Rule #1 – User Account Created

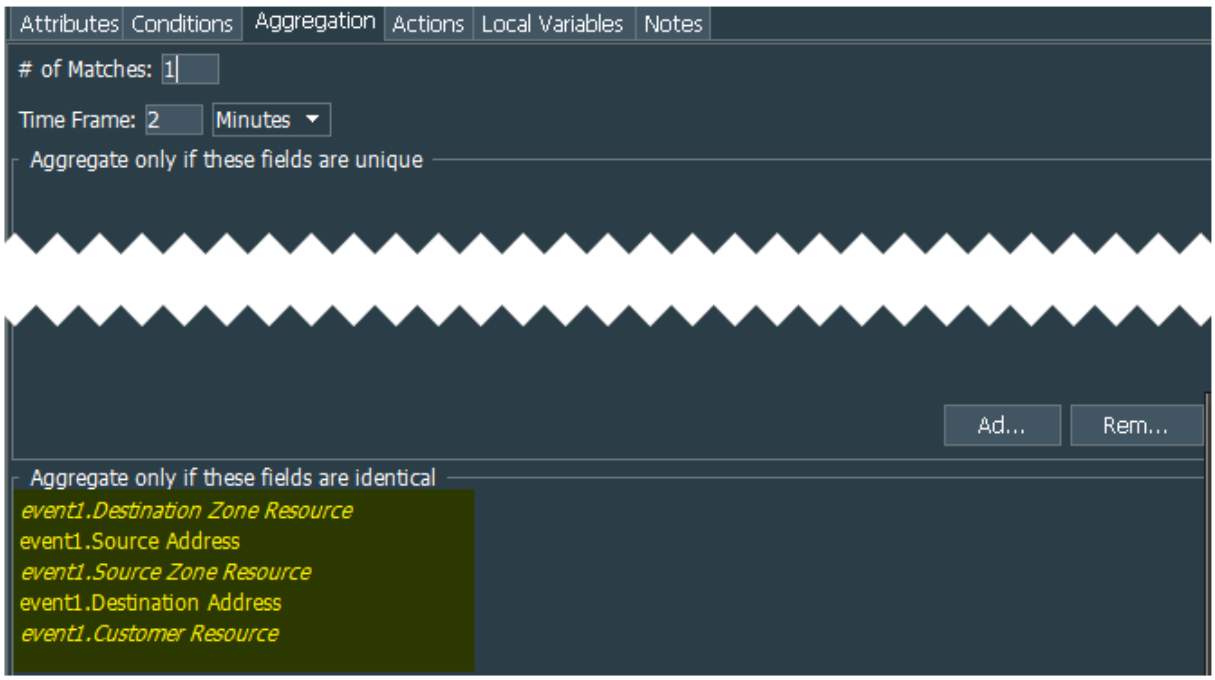
1. Vytvoříme pravidlo *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC4_[Prijmeni]_Communication_with_Suspicious_Address*
   a. Attributes



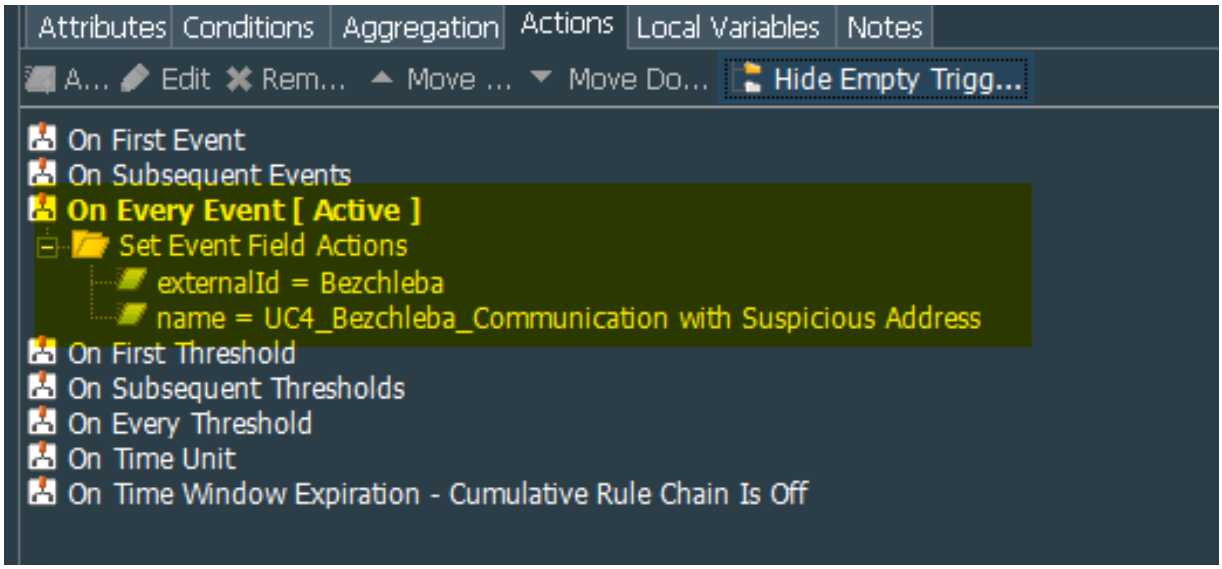
b. Conditions



c. Aggregation



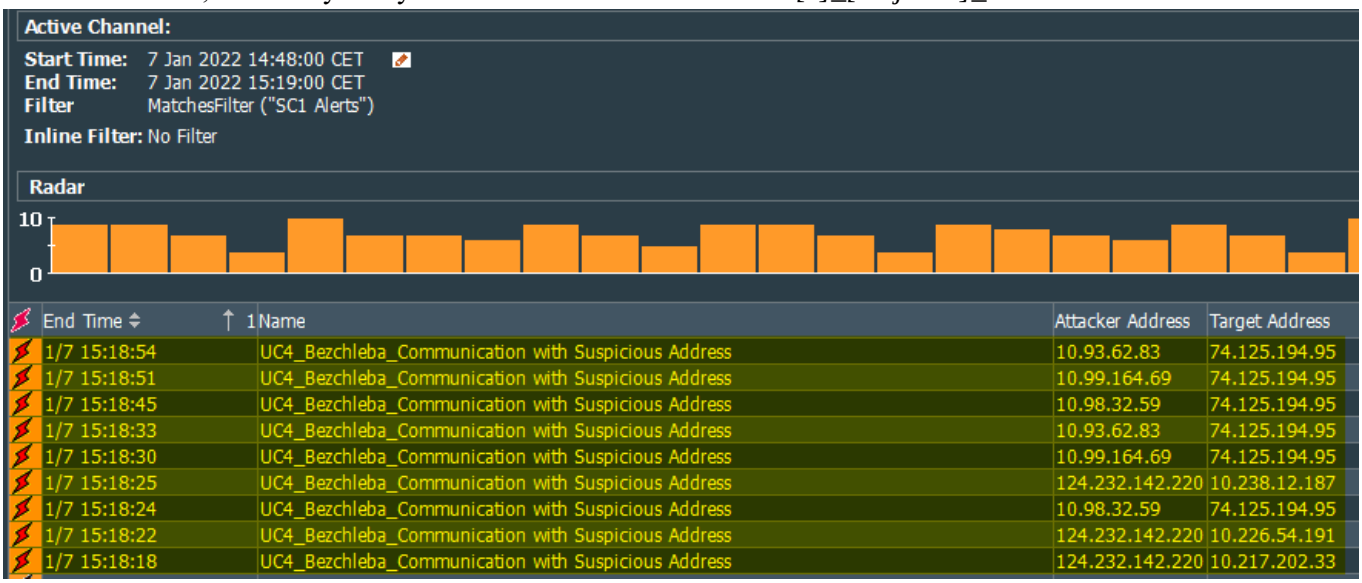
d. Actions



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.

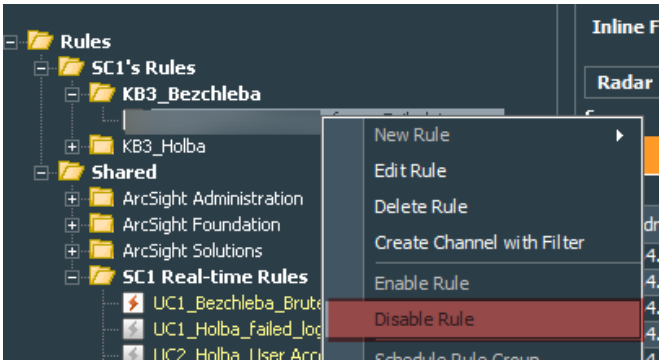
2.2.4 Ověření funkčnosti pravidla

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

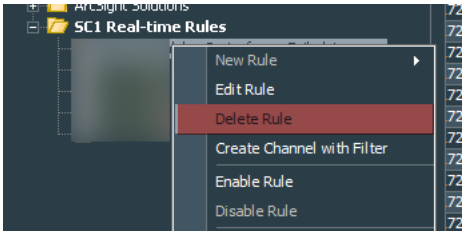


2.2.5 Úklid ESM

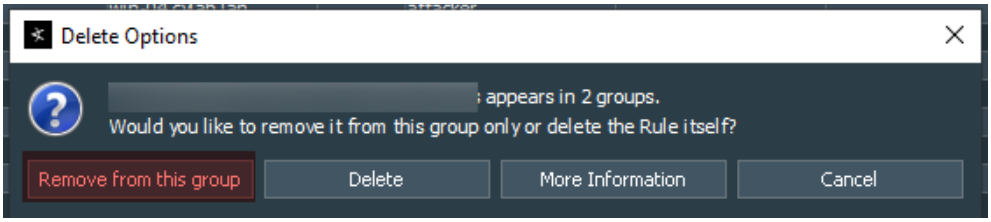
1. Vypneme pravidla:
    a. *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC4_[Prijmeni]_Communication_with_Suspicious_Address*



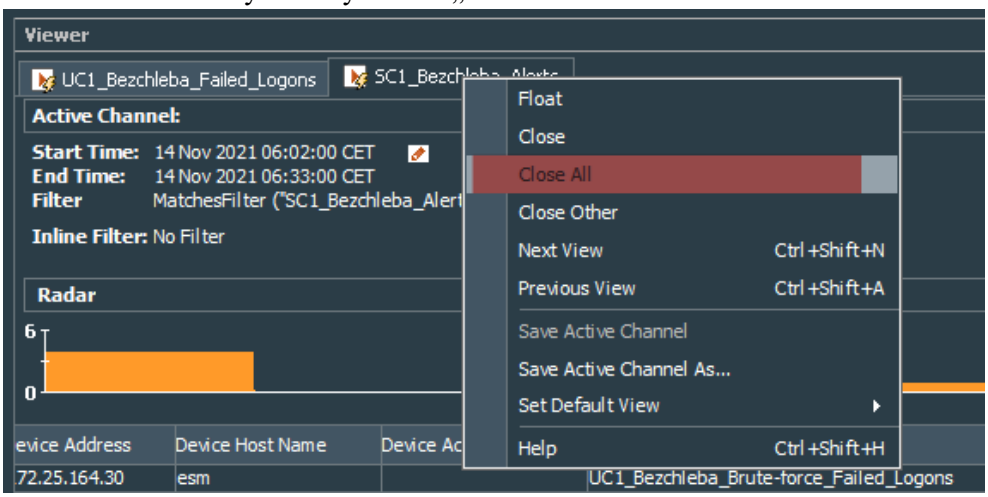
2. Pravidlo odlinkujeme z SC[x] Real-time Rules.



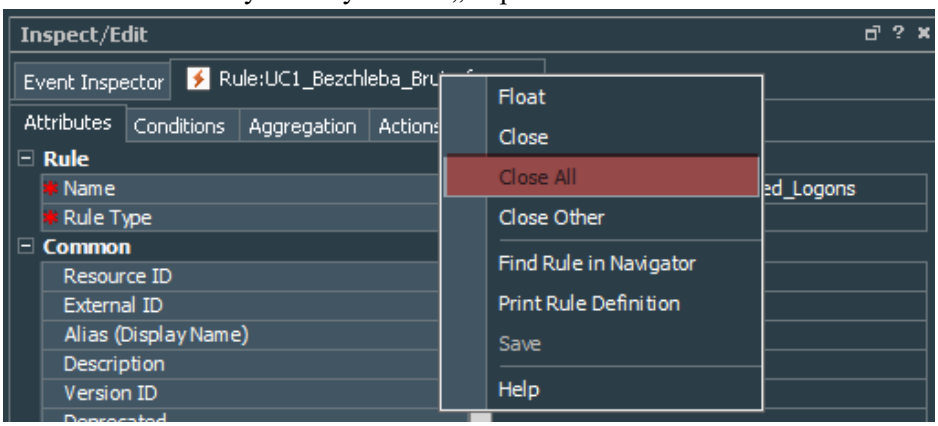
Pozor!!! Zvolíme – „Remove from this group“. Pokud bychom zvolil možnost „Delete“, tak pravidlo se celé smaže.



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/