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 – Brute Force Attack

Metodický list

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

Recenzent: Ing. Peter Jankovský

Rok vydání: 2023

Obsah

Cíle 2

Dovednosti 2

Kontrolní otázky 2

Pracovní prostředí 2

1 Průběh výuky 3

2 Zadání 4

2.1 ČÁST Logger 4

2.2 ČÁST ESM 5

2.2.1 Filter – UC1_[Prijmeni]_Failed_Logons 5

2.2.2 Active Channel – UC1_[Prijmeni]_Failed_Logons 5

2.2.3 Rule – UC1_[Prijmeni]_Brute-force_Failed_Logons 6

2.2.4 Filters – SC1_[Prijmeni]_Alerts 7

2.2.5 Active Channel – SC1_[Prijmeni]_Alerts 8

2.2.6 Úklid ESM 9

Seznam použitých zdrojů 11

Cíle

- Žák definuje techniku BruteForce.
- Žák rozlišuje podmetody MITRE BRUTEFORCE.
- Žák dokáže pojmenovat a popsat metody obrany proti BruteForce Attack.

Dovednosti

- Žák navrhne a aplikuje filtr pro vyhledání záznamů v ArcSight Loggeru související z BruteForce útokem.
- Žák interpretuje výsledky vyhledávání.
- Žák navrhne a aplikuje filtr a pravidla pro automatické vyhodnocování událostí v nástroji ArcSight ESM.

Kontrolní otázky

- Jaké máme metody obrany?
- V jaké fázi útoku (Attack Life Cycle) se nachází v tuto chvíli útočník?

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
- Web: https://www.logbinder.com/

[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: 10 událostí za **sekundu**
    b. Část ESM: 100 událostí za **minutu**
5. Spusťte následující provoz a nechte jej běžet:
    a. dhcp_3h.events
    b. dns_3h.events
    c. winc_3h.events
    d. **UC1_Bruteforce-Attack\bad_passwd.events**
    e. **UC1_Bruteforce-Attack\bad_user.events**

2 Zadání

2.1 ČÁST Logger

Zjistěte, zda nedošlo v poslední době k neúspěšnému přihlášení na nějakou stanici. Pokud ano, může se jednat o útok Brute-force Attack. Proveď proto další šetření

1. Na které stanice probíhá potenciální útok?

```
categoryBehavior = /Authentication/Verify AND categoryOutcome = /Failure | TOP
destinationAddress, destinationHostName
```

   Správná odpověď: win-01.cylab.lan, win-02.cylab.lan, win-03.cylab.lan, win-04.cylab.lan, win-05.cylab.lan

2. Z kterých stanic probíhá potenciální útok?

```
categoryBehavior = /Authentication/Verify AND categoryOutcome = /Failure | TOP
sourceAddress, sourceHostName
```

   Správná odpověď: dmz-rc1.jcekb.cz

3. Pod jakými účty se útočník snaží přihlásit?

```
categoryBehavior = /Authentication/Verify AND categoryOutcome = /Failure | TOP
destinationAddress, destinationHostName, destinationUserName
```

   Správná odpověď: pparker, attacker

4. Zjisti, jestli z uživatelských účtů, pod kterými probíhal útok nebylo úspěšné přihlášení.

```
categoryBehavior = /Authentication/Verify AND categoryOutcome = /Success AND
(destinationUserName=pparker OR destinationUserName=attacker)
```

   Správná odpověď: Nebylo

5. Pokročilejší - Zjisti, jestli se jedná o neúspěšné zadání hesla, nebo o neexistenci uživatelského účtu.

```
categoryBehavior = /Authentication/Verify AND categoryOutcome = /Failure | top
destinationUserName, deviceCustomString1
```

   Správná odpověď:

   pparker – 0xC000006A – Nesprávné heslo

   attacker – 0xC0000064 – Uživatelský účet neexistuje

   Zdroj:

   https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

2.2 ČÁST ESM

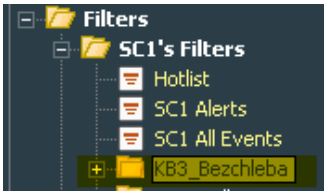
Napište a aplikujte v programu ESM pravidla, která odhalí pokus o Brute-force Attack ve vaší síti.

1. Žák musí vytvořit
    a. Filter
    b. Active Channel
    c. Rules

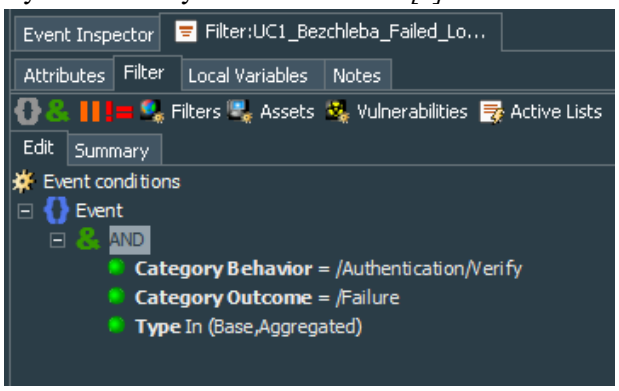
Práci je nutné ukončit "Úklidem ESM"

2.2.1 Filter – UC1_[Prijmeni]_Failed_Logons

1. Každý student si vytvoří novou složku *Filters -> SC[x]'s Filters -> KB[x]_[Prijmeni]*
   Pozn.: Žáci musí postupně. Jeden po druhém!

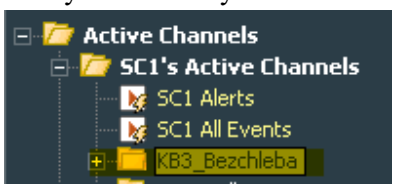


2. Vytvoříme nový filtr *Filters -> SC[x]'s Filters -> KB[x] [Prijmeni] -> UC1_[Prijmeni]_Failed_Logons*

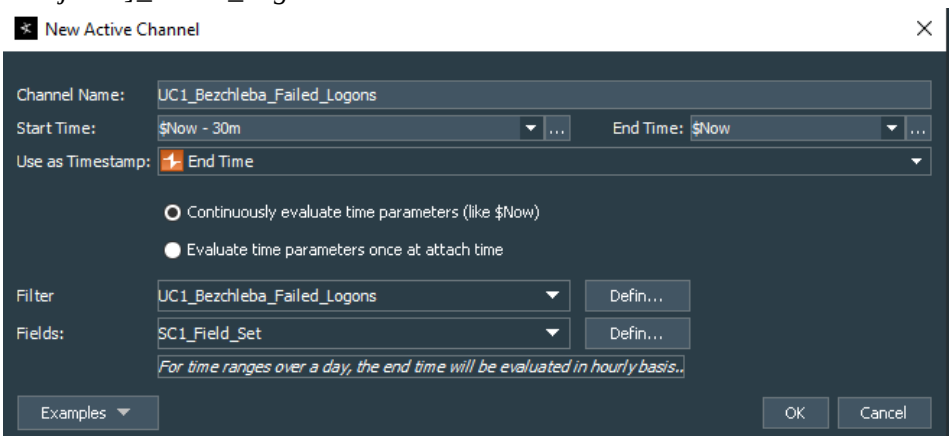


2.2.2 Active Channel – UC1_[Prijmeni]_Failed_Logons

1. Každý student si vytvoří novou složku v *Active Channels -> SC[x]'s Active Channels -> KB[x]_[Prijmeni]*



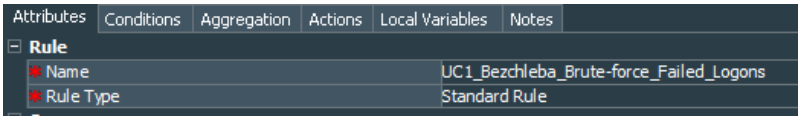
2. Vytvoříme nový aktivní kanál *Active Channels -> SC[x]'s Active Channels -> KB[x]_[Prijmeni] -> UC1_[Prijmeni]_Failed_Logons*

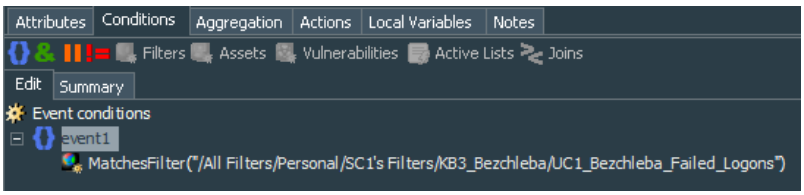


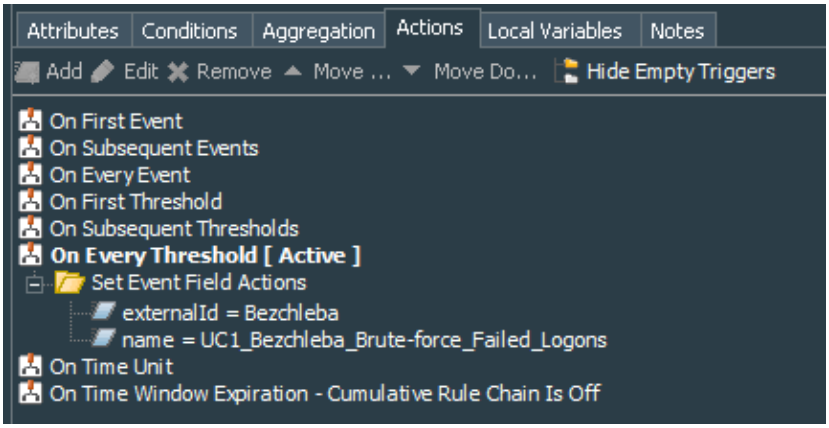
3. Seznámíme studenty s ovládacími prvky Active Channel.

2.2.3 Rule – UC1_[Prijmeni]_Brute-force_Failed_Logons

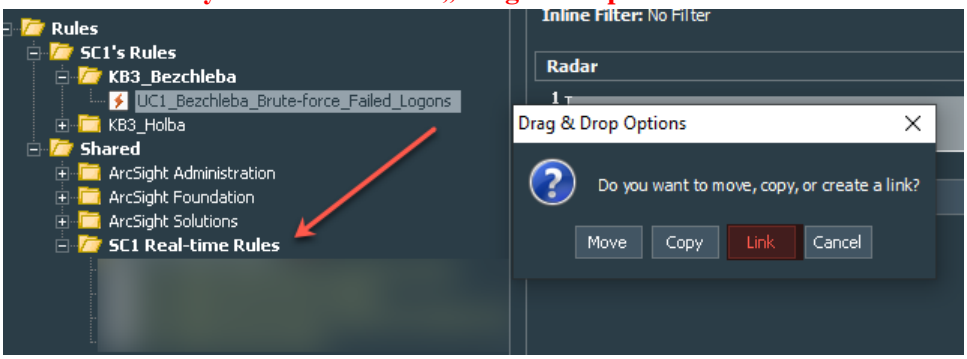
1. Vytvoříme pravidlo *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC1_[Prijmeni]_Brute-force_Failed_Logons*







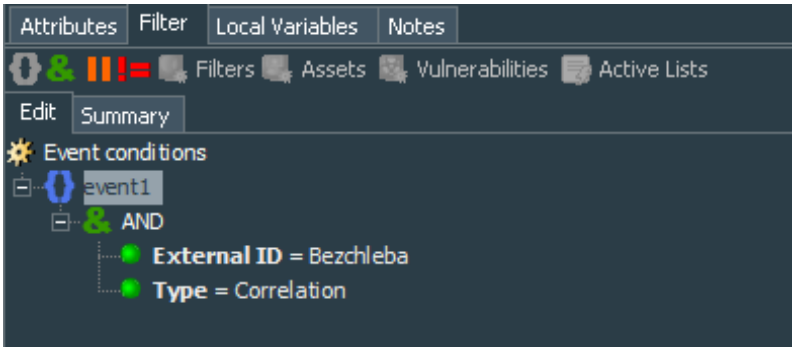
2. Pravidlo přesuneme metodou „Drag & Drop“ do složky *Rules -> Shared -> SC[x] Real-Time Rules*
    a. **Ve vyskakovacím okně „Drag & Drop zvolím Link.**



3. Pravidlo je aktivní a začíná korelovat.

2.2.4 Filters – SC1_[Prijmeni]_Alerts

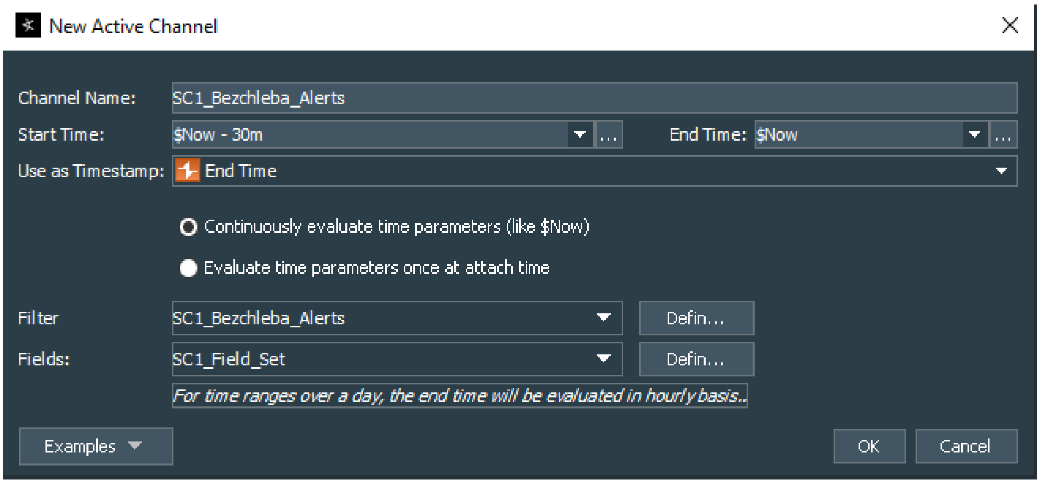
1. Vytvoříme filtr *Filters -> SC[x]'s Filters -> KB[x] [Prijmeni] -> SC[x]_[Prijmeni]_Alerts*



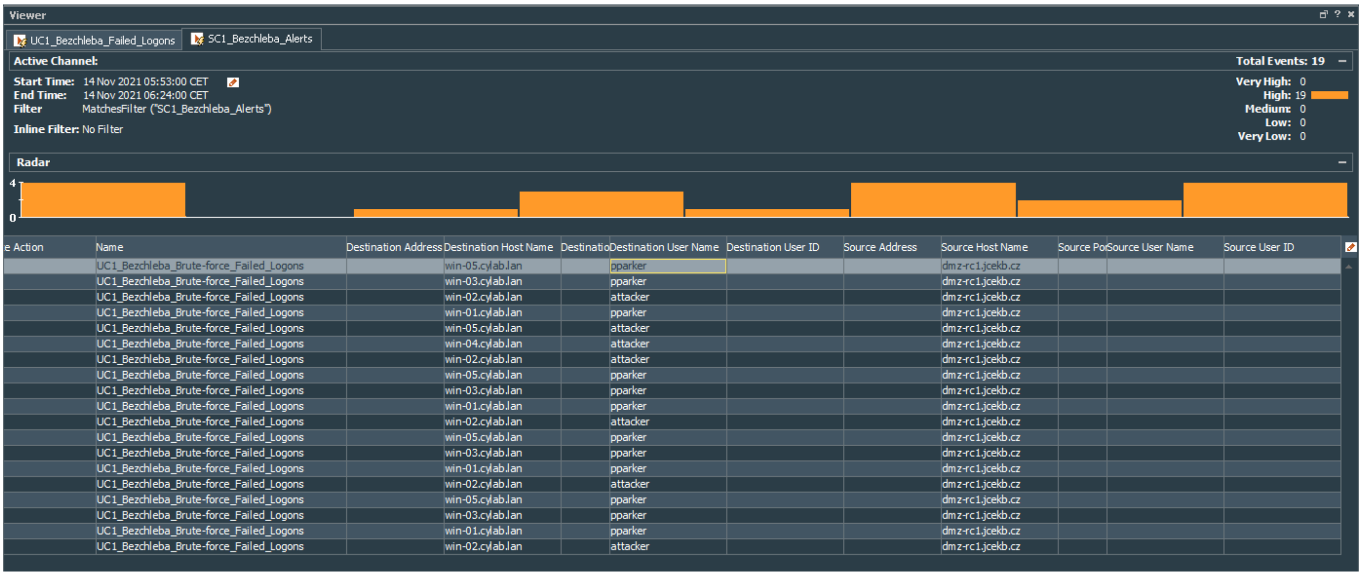
2.2.5 Active Channel – SC1_[Prijmeni]_Alerts

V tomto aktivním kanále zobrazíme alerty.

1. Vytvoříme nový aktivní kanál *Active Channels -> SC[x]'s Active Channels -> KB[x]_[Prijmeni] -> SC[x]_Alerts*

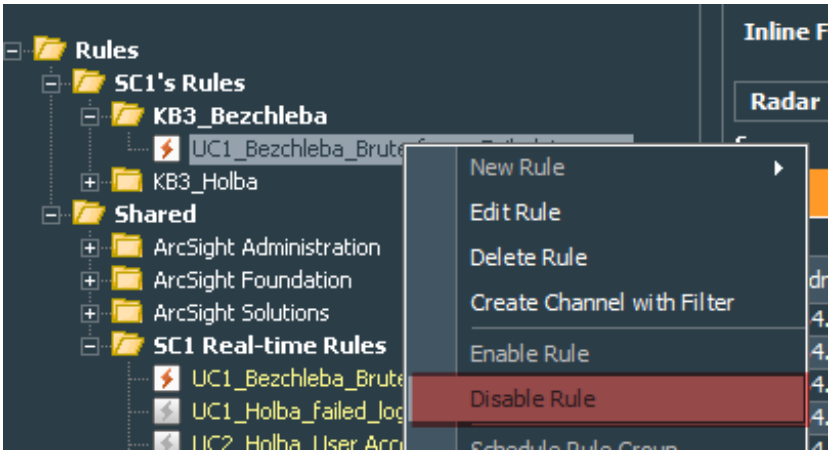


Pokud jsme postupovali správně, začnou se v aktivním kanále postupně zobrazovat alerty.

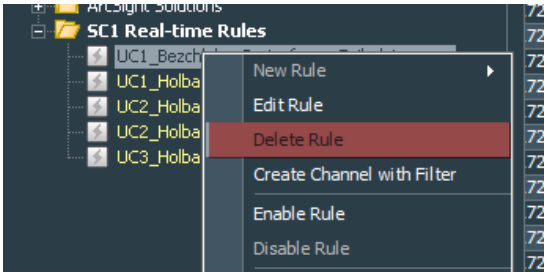


2.2.6 Úklid ESM

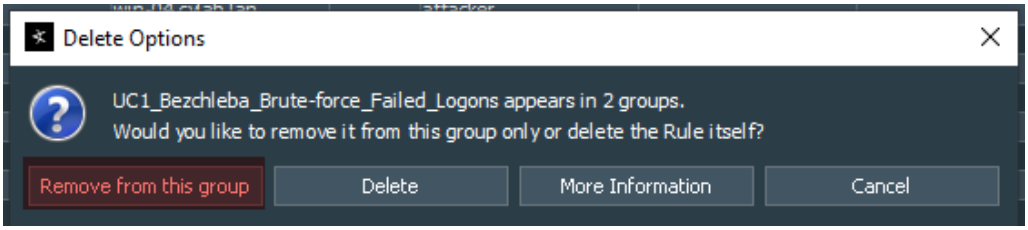
1. Vypneme pravidlo *Rules -> SC[x]'s Rules -> KB[x]_[Prijmeni] -> UC1_[Prijmeni]_Brute-force_Failed_Logons*



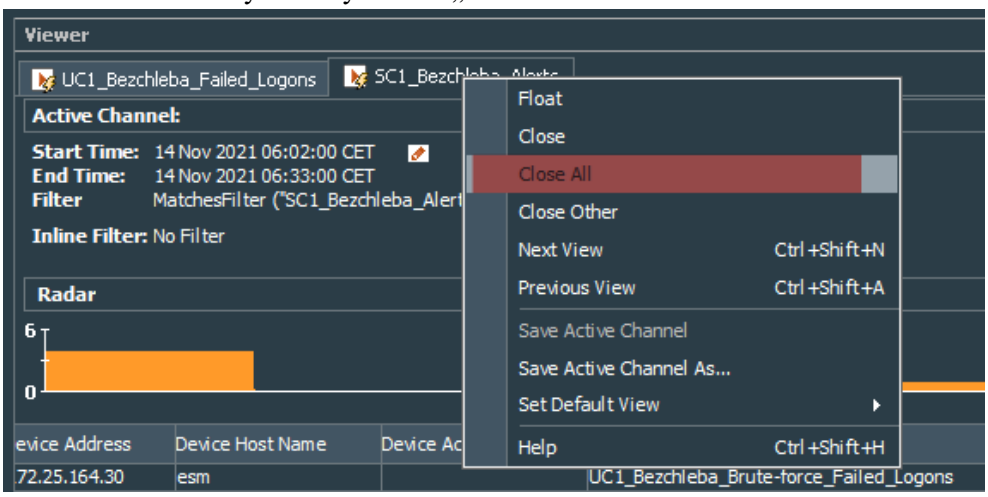
2. Pravidlo odlinkujeme z SC[x] Real-time Rules.



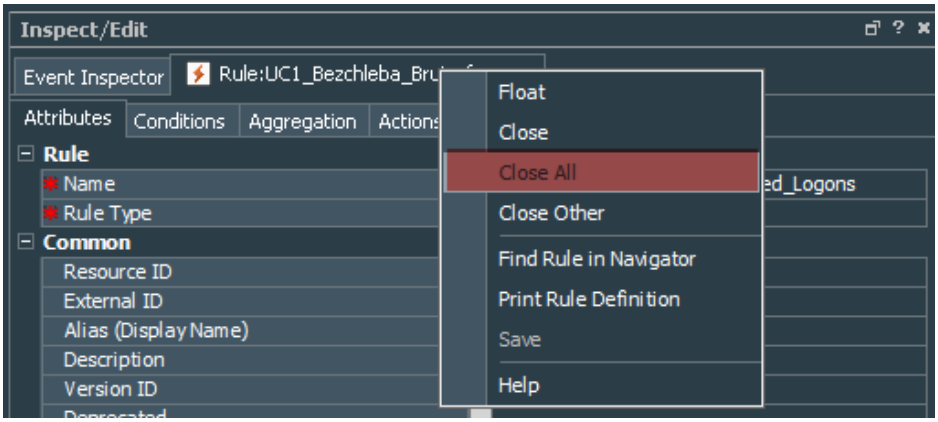
Pozor!!! Zvolíme – „Remove from this group". Pokud bychom zvolil možnost „Delete", tak pravidlo se celé smaže.



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/